VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE Č. 2

ve smyslu § 98 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů
(dále jen „ZZVZ“ či „zákon“)

1. Identifikační údaje o veřejné zakázce a o zadavateli

1.1. Identifikační údaje o veřejné zakázce

Název veřejné zakázky	**Zajištění kybernetické bezpečnosti Střední školy Edvarda Beneše Břeclav, příspěvková organizace**
Režim veřejné zakázky	nadlimitní
Druh zadávacího řízení	otevřené řízení
Druh veřejné zakázky	dodávky

1.2. Identifikační údaje zadavatele

Název	Střední škola Edvarda Beneše Břeclav, příspěvková organizace
Sídlo	nábř. Komenského 1126/1, 690 25, Břeclav
IČO	60680342
Zastoupené	Mgr. Jiřím Uherem, ředitelem
Právní forma	příspěvková organizace
Profil zadavatele	https://zakazky.krajbezkorupce.cz/profile_display_138.html

1.3. Identifikační údaje smluvního zástupce zadavatele ve smyslu § 43 zákona

Název	Advokátní kancelář Petráš Rezek s.r.o.
Sídlo	Opletalova 1525/39, Nové Město, 110 00 Praha 1
IČO	07417641
Zastoupený/á	Mgr. Filipem Petrášem, společníkem a jednatelem
Právní forma	společnost s ručením omezeným
Kontaktní osoba	Mgr. Michal Uherek Verejne.zakazky@petrasrezek.cz
na základě pověření společnosti	
Název	Regionální rozvojová agentura Východní Moravy
Sídlo	třída Tomáše Bati 5146, 760 01 Zlín
IČO	45659176
Zastoupený/á	RNDr. Otakarem Prudilem, ředitelem

2. Předmět vysvětlení zadávací dokumentace

Zadavatel na základě žádosti dodavatele ze dne 06.05.2025 poskytuje následující vysvětlení zadávací dokumentace k výše uvedené veřejné zakázce.

Dotaz č. 1:
Zadavatel soustředil technické podmínky vymezující předmět veřejné zakázky do Přílohy č. 1 s názvem Technická specifikace. Přestože je třeba bezvýjimečně chápat splnění vymezených minimálních požadavků parametrů nabízených zařízení jako jednu z podmínek účasti, připouští zadavatel uvedení u každého povinného parametru i možnost NE, tj. že konkrétní parametr není splněn. Chápe uchazeč správně, že uvedení „NE“ u kteréhokoliv požadavku má za důsledek označení nabídky zadavatelem jako nevyhovující co do splnění všech podmínek účasti s důsledkem jejího vyřazení ze zadávacího řízení? Pokud je tomu tak, nechť zadavatel vysvětlí, proč připouští i možnost nesplnění parametru, protože v takovém případě by nemělo smysl vůbec nabídku podávat. Nebo zadavatel předpokládá, že se v nabídce objeví i vyplněná možnost NE a pak bude posuzovat, zda nesplnění parametru nějak „odpustí“ a tím zvýhodní takového účastníka oproti jiným, kteří, vědomi si nesplnění povinného parametru, vůbec nabídku nepodali?

Odpověď na dotaz č. 1:
Účastník je povinen v příloze č. 1 zadávací dokumentace – Technická specifikace vyplnit označené pole, a to především uvést hodnotu ANO či NE u jednotlivých požadavků. Uvede-li účastník hodnotu ANO, potvrzuje tím zadavateli schopnost splnění požadavku. Uvede-li účastník hodnotu NE, uvádí tím, že není schopný uvedený požadavek splnit. Za nesplnění požadavku bude účastník ze zadávacího řízení vyloučen.
Zadavatel požaduje vyplnění hodnoty k jednotlivým požadavkům z důvodu potvrzení, zda účastník požadavek splňuje či nikoli.

Znění k následujícím dotazům:
Vzhledem, k tomu že jsme nalezli v Technické specifikaci několik minimálních požadavků, které lze jednoznačně považovat za nepřímé odkazy na určité dodavatele či výrobky, upozorňujeme v dalším textu na jejich konkrétní výskyt a žádáme zadavatele, aby alespoň tyto vyspecifikované minimální parametry odůvodnil ve smyslu § 89 odst. 5 ZZVZ případně je upravil. Domníváme se, že je nelze věrohodně odůvodnit předmětem zakázky. Zadavatel sice uvedl v zadávací dokumentaci v kap. 10, že umožňuje u každého takového odkazu možnost nabídnout rovnocenné řešení, ale v následné argumentaci komentujeme, že požadavky zadavatele odpovídají jen specifikaci jednotlivých produktů konkrétních výrobců a nejsou v souladu se ZZVZ. Jejich povinné splnění tak znemožňuje účast některých subjektů v tomto zadávacím řízení a v rovné hospodářské soutěži. Současně se domníváme, že na základě našich implementačních zkušeností z obdobných projektů zajištění kybernetické bezpečnosti pro podobně velká školská zařízení, uvedení některých požadavků v technické specifikaci směřuje ať již vědomě či nevědomě na omezení hospodářské soutěže a jsme přesvědčeni, že nejsou pro dané řešení kybernetické bezpečnosti bezpodmínečně nutné, respektive mohou být pro daný projekt a jeho cíl nepřiměřené nebo neúměrně nákladné. Zadavatel by měl zvážit jejich úpravu i s ohledem na skutečné potřeby zadavatele.
Jedná se zejména o tyto požadavky:

Dotaz č. 2:
Požadavek na fyzické vlastnosti virtualizačních serverů a backup serveru
Požadavek na displej zobrazující IP adresu a chybové stavy na čelní straně serveru je dle našeho názoru nepřiměřeně specifický a de facto odpovídá technickému řešení konkrétních výrobců (např. Dell). Tím může docházet k diskriminaci dodavatelů využívajících alternativní metody monitorování. Žádáme o vysvětlení, zda je tento displej nezbytný pro plnění účelu zakázky (zajištění kybernetické bezpečnosti), nebo zda lze požadovanou funkcionalitu řešit ekvivalentními prostředky (§ 36 odst. 2 ZZVZ).
Z naší zkušenosti mohou pro daný účel sloužit jiné nástroje a u čelná strany serveru mohou stačit např. stavové LED diody.

Odpověď na dotaz č. 2:
Zadavatel trvá na požadavku vizuální identifikace IP adresy a chybových stavů na čelní straně serveru, ale upřesňuje, že tento požadavek lze splnit pomocí různých technologických řešení, nikoliv pouze prostřednictvím LCD displeje. Požadovanou funkcionalitu lze zajistit i ekvivalentními prostředky, které umožní rychlou a jednoznačnou vizuální identifikaci serverů a jejich stavů. Tento požadavek má přímou vazbu na naplnění cílů zakázky v oblasti zajištění kybernetické bezpečnosti.
1. Legislativní opory požadavku
Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
§ 4 odst. 1 - "Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru."

- Rychlá vizuální identifikace serverů a jejich stavu přispívá k zajištění dostupnosti a spolehlivosti služeb díky zkrácení doby potřebné pro lokalizaci a řešení problémů.

§ 5 odst. 2 písm. e) - Povinná osoba je povinna "zavést vhodná bezpečnostní opatření, aktualizovat je a pravidelně vyhodnocovat jejich účinnost."

- Rychlá vizuální identifikace serverů představuje vhodné bezpečnostní opatření pro zajištění rychlé reakce při řešení bezpečnostních incidentů.

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních
§ 13 - Zajištění dostupnosti
(2) Povinná osoba dále v rámci řízení dostupnosti

a) zajistí dostupnost informačního a komunikačního systému tak, aby byl v případě dopadů kybernetické bezpečnostní události na dostupnost zachován provoz informačního a komunikačního systému alespoň v minimálním rozsahu určeném vybranou osobou, a tím zajistit dostupnost primárních aktiv,

- Rychlá vizuální identifikace serverů zkracuje dobu potřebnou pro lokalizaci a řešení problémů, čímž přispívá k zachování provozu systémů.

§ 16 - Bezpečnost provozu

(2) Povinná osoba v rámci zajištění bezpečnosti provozu informačního a komunikačního systému
c) zajistí včasné odhalení technických a bezpečnostních incidentů,

- Vizuální identifikace serverů a jejich stavu přispívá k včasnému odhalení technických a bezpečnostních incidentů.

ISO/IEC 27001:2022

Příloha A.5.30 - Dostupnost informací

- Vyžaduje implementaci opatření pro zajištění dostupnosti informací a zpracování informací.

Příloha A.8.9 - Monitorování

- Požaduje implementaci systémů pro monitoring a zaznamenávání událostí.

Směrnice NIS2 (EU) 2022/2555

Článek 21 - Opatření k řízení rizik kybernetické bezpečnosti
2. Opatření uvedená v odstavci 1 zahrnují přinejmenším:
i) používání a vývoj postupů pro zachování dostupnosti služeb;

- Rychlá vizuální identifikace serverů představuje účinný postup pro zachování dostupnosti služeb díky zkrácení doby potřebné pro lokalizaci a řešení problémů.

2. Bezpečnostní důvody pro trvání na požadavku vizuální identifikace

2.1 Rychlá reakce na bezpečnostní incidenty

Rychlá vizuální identifikace serverů a jejich stavu je klíčová pro efektivní řešení bezpečnostních incidentů:

- **Minimalizace MTTR (Mean Time To Resolve)** - Zkrácení doby mezi identifikací incidentu a jeho vyřešením díky rychlé lokalizaci problematického serveru.
- **Prevence zásahu do nesprávného serveru** - Jednoznačná identifikace serveru minimalizuje riziko zásahu do nesprávného zařízení při řešení incidentu.
- **Rychlá identifikace fyzicky kompromitovaných serverů** - Možnost rychle identifikovat servery, které vykazují známky fyzického narušení.
- **Efektivnější koordinace při řešení komplexních incidentů** - Při řešení komplexních incidentů vyžadujících zásah více techniků umožňuje jasnou komunikaci o konkrétních zařízeních.

2.2 Prevence insider threats a neoprávněné manipulace

Jasná vizuální identifikace serverů přispívá k prevenci insider threats:

- **Zvýšení transparentnosti při fyzickém přístupu** - Jasné označení a zobrazení stavu serverů zvyšuje transparentnost při fyzickém přístupu k zařízením.
- **Snadnější detekce neautorizované manipulace** - Viditelné označení serverů usnadňuje detekci neautorizované manipulace s hardware.
- **Prevence záměny hardwaru** - Jasná identifikace ztěžuje záměrné zaměnění hardwaru při insider útoku.
- **Podpora pro fyzické audity** - Usnadnění fyzických auditů datového centra díky jasné identifikaci všech zařízení.

2.3 Zajištění dostupnosti služeb při mimořádných situacích

V případě mimořádných situací je rychlá identifikace serverů kritická:

- **Rychlá evakuace kritických serverů** - V případě fyzického ohrožení (požár, povodeň) umožňuje rychlou identifikaci kritických serverů pro prioritní záchranu.
- **Efektivnější disaster recovery** - Při obnově po havárii umožňuje rychlejší identifikaci a zprovoznění klíčových serverů.
- **Podpora pro nouzové postupy** - Usnadnění implementace nouzových postupů díky jednoznačné identifikaci zařízení i bez přístupu k dokumentaci.
- **Minimalizace závislosti na centrálních monitorovacích systémech** - Možnost identifikace serverů i při výpadku centrálních monitorovacích systémů.

2.4 Zvýšení efektivity bezpečnostních auditů a kontrol

Vizuální identifikace serverů zvyšuje efektivitu bezpečnostních auditů a kontrol:

- **Zrychlení fyzických bezpečnostních auditů** - Možnost rychlejšího provedení fyzických bezpečnostních auditů díky jasné identifikaci zařízení.

- **Podpora pro inventarizaci aktiv** - Usnadnění inventarizace fyzických aktiv, což je klíčový požadavek kybernetické bezpečnosti.
- **Verifikace souladu fyzické a logické topologie** - Možnost snadno ověřit, zda fyzické umístění serverů odpovídá dokumentované logické topologii.
- **Kontrola neoprávněného hardware** - Snazší identifikace neoprávněně přidaného hardware do racků.

3. Technické zdůvodnění požadavku a akceptovatelná ekvivalentní řešení

3.1 Klíčové funkční požadavky na vizuální identifikaci

Zadavatel definuje následující klíčové funkční požadavky na systém vizuální identifikace:

- **Jasná identifikace serveru** - Systém musí poskytovat jednoznačnou identifikaci konkrétního serveru včetně jeho IP adresy.
- **Zobrazení chybových stavů** - Systém musí poskytovat jasnou vizuální indikaci chybových stavů.
- **Viditelnost z čelní strany racku** - Informace musí být viditelné z čelní strany racku bez nutnosti otevírání dveří nebo manipulace se serverem.
- **Čitelnost na vzdálenost minimálně 1 metr** - Informace musí být čitelné na vzdálenost minimálně 1 metr, aby bylo možné rychle identifikovat server z uličky datového centra.
- **Funkčnost i při částečném výpadku napájení** - Základní identifikace musí být možná i při výpadku hlavního napájení serveru.

3.2 Akceptovatelná ekvivalentní řešení na trhu

Zadavatel uznává, že požadované funkce lze realizovat různými technologickými řešeními dostupnými na trhu, například:

3.2.1 Displeje (LCD, OLED, E-ink)

- **LCD displeje** - Tradiční řešení
- **OLED displeje** - Řešení s vyšším kontrastem a lepší čitelností z více úhlů
- **E-ink displeje** - Řešení s nízkou spotřebou vhodné pro zobrazení statických informací

3.2.2 Pokročilé LED systémy

- **Programovatelné LED matice** - Pokročilé systémy LED matic, které dokáží zobrazit základní alfanumerické informace
- **Barevně kódované LED systémy** - Systémy využívající kombinace barev a pozic LED pro kódování informací
- **LED displeje s posunem textu** - LED displeje umožňující zobrazení posuvného textu s informacemi

3.2.3 Kombinovaná řešení

- **QR kódy s LED indikací** - Kombinace statického QR kódu (pro identifikaci serveru) s dynamickou LED indikací stavu
- **NFC/RFID tagy s vizuální indikací** - Kombinace NFC/RFID tagů pro identifikaci s vizuálním systémem pro indikaci stavu
- **Rozšířená identifikační štítky s integrovanými LED** - Štítky s dynamicky se měnícími informacemi

3.3 Pro shora uvedené existuje na trhu řešení od více jak 10 různých výrobců.

4. Praktické scénáře využití vizuální identifikace v kontextu kybernetické bezpečnosti

4.1 Scénář: Rychlá reakce na podezření na malware

Pokud bezpečnostní monitoring detekuje podezřelou aktivitu na serveru, vizuální identifikace umožňuje:

- Rychlé lokalizování fyzického serveru v racku bez nutnosti procházet dokumentaci
- Okamžité ověření, zda server vykazuje nějaké neobvyklé chování (vysoké vytížení, neobvyklá síťová aktivita)
- Rychlou fyzickou izolaci serveru od sítě v případě potřeby

4.2 Scénář: Incident response během rozsáhlého útoku

Při řešení rozsáhlého bezpečnostního incidentu:

- Rychlá identifikace všech potenciálně zasažených serverů
- Paralelní práce více členů incident response týmu díky jednoznačné identifikaci serverů
- Možnost fyzické izolace kompromitovaných serverů bez nutnosti přístupu do administrativního rozhraní

4.3 Scénář: Pravidelný fyzický audit datového centra

Při provádění pravidelných bezpečnostních auditů:

- Rychlá kontrola, zda všechny servery v racku odpovídají inventarizaci
- Rychlá detekce serverů vykazujících neočekávaný stav
- Efektivnější kontrola fyzického zabezpečení jednotlivých serverů

4.4 Scénář: Obnova po fyzickém incidentu

V případě fyzického incidentu (např. výpadek klimatizace, částečný výpadek napájení):

- Rychlá identifikace serverů, které byly incidentem zasaženy

- Prioritizace obnovy kritických systémů na základě jejich jasné identifikace
- Možnost identifikace serverů i při částečném výpadku napájení nebo síťové konektivity

5. Výrobci a dostupná řešení na trhu

5.1 Hlavní výrobci s řešeními splňujícími požadavek

Zadavatel zdůrazňuje, že na trhu existuje široká škála výrobců, kteří nabízejí řešení splňující požadavek na vizuální identifikaci serverů.

5.2 Specializovaní výrobci rozšiřujících řešení

Pro výrobce serverů, kteří standardně nenabízejí pokročilou vizuální identifikaci, existují specializovaní výrobci doplňkových řešení.

6. Řešení potenciálních námitek

6.1 Námitka: "Požadavek zvýhodňuje pouze některé výrobce"

Odpověď: Jak je uvedeno v sekci 5, požadavek lze splnit řešeními od široké škály výrobců, ať už prostřednictvím integrovaných displejů, pokročilých LED systémů nebo kombinovaných řešení. Zadavatel akceptuje různé technologické přístupy, které splní definované funkční požadavky.

6.2 Námitka: "Požadavek je možné řešit centrálním monitoringem"

Odpověď: Centrální monitoring je důležitým doplňkem, ale nenahrazuje potřebu rychlé fyzické identifikace serverů přímo v datovém centru. V případě fyzických incidentů, při narušení síťové konektivity nebo při podezření na kompromitaci monitorovacího systému je fyzická identifikace serverů kritická.

6.3 Námitka: "Standardní LED indikace je dostačující"

Odpověď: Standardní LED indikace (power, disk, síť) neumožňuje jednoznačnou identifikaci serveru včetně jeho IP adresy a neposkytuje dostatečně detailní informaci o chybových stavech. Zadavatel však akceptuje pokročilé LED systémy, které tyto informace dokáží komunikovat.

7. Závěr

Zadavatel trvá na požadavku vizuální identifikace IP adresy a chybových stavů na čelní straně serverů jako na důležitém prvku zajištění kybernetické bezpečnosti, který přispívá k rychlé reakci na bezpečnostní incidenty, minimalizaci doby výpadku služeb a efektivní správě fyzických aktiv.

Zadavatel však upřesňuje, že tento požadavek lze splnit různými technologickými řešeními, nikoliv pouze LCD displejem. Akceptovatelná jsou ekvivalentní řešení včetně pokročilých LED systémů, kombinovaných řešení s QR/NFC/RFID technologiemi nebo jiných inovativních přístupů, pokud splní klíčové funkční požadavky na jasnou identifikaci serveru a zobrazení jeho stavu z čelní strany racku.

Zadavatel konstatuje, že tento požadavek je splnitelný širokou škálou výrobců na trhu a nepředstavuje nepřiměřené omezení hospodářské soutěže. Technická specifikace umožňuje široké spektrum řešení při zachování požadované funkcionality v souladu s § 36 odst. 1 ZZVZ.

Dotaz č. 3:

Požadavek u virtualizačních serverů a u backup serveru na mobilní aplikaci

Požadavek na přístup do cloudového portálu výrobce serverů a ovládání grafické konzole pro správu a monitorování serverů také přes mobilní aplikace dostupné pro iOS a Android, není v kontextu správy daných serverů obvyklý a omezuje soutěž na dodavatele s proprietárními řešeními. Žádáme o odstranění tohoto požadavku včetně odůvodnění, jak konkrétně přispívá k naplnění cílů zakázky.

Z naší zkušenosti je požadavek na mobilní aplikaci pro iOS a Android pro dané použití nadbytečný.

Odpověď na dotaz č. 3:

Zadavatel trvá na požadavku přístupu do cloudového portálu výrobce serverů a ovládání grafické konzole pro správu a monitorování serverů také přes mobilní aplikace dostupné pro iOS a Android, a to z důvodů souvisejících s kybernetickou bezpečností a zvýšením efektivity reakce na bezpečnostní incidenty. Tento požadavek má přímou vazbu na naplnění cílů zakázky v oblasti zajištění kybernetické bezpečnosti a je v souladu s moderními trendy v oblasti správy IT infrastruktury a reaktivní kybernetické bezpečnosti.

1. Legislativní opory požadavku

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

§ 4 odst. 1 - "Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru."

- Mobilní přístup ke správě serverů přispívá k zajištění dostupnosti a spolehlivosti služeb díky možnosti rychlejší reakce na bezpečnostní incidenty.

§ 5 odst. 2 písm. e) - Povinná osoba je povinna "zavést vhodná bezpečnostní opatření, aktualizovat je a pravidelně vyhodnocovat jejich účinnost."

- Mobilní přístup představuje vhodné bezpečnostní opatření umožňující rychlou reakci na bezpečnostní události i mimo standardní pracovní dobu.

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních

§ 13 - Zajištění dostupnosti

(2) Povinná osoba dále v rámci řízení dostupnosti

e) implementuje opatření pro zajišťování dostupnosti, kterými zajistí odolnost informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům, které by mohly snížit dostupnost,

- Mobilní přístup ke správě serverů zvyšuje odolnost informačního systému díky možnosti okamžité reakce na incidenty.

§ 16 - Bezpečnost provozu

(2) Povinná osoba v rámci zajištění bezpečnosti provozu informačního a komunikačního systému

c) zajistí včasné odhalení technických a bezpečnostních incidentů,

- Mobilní přístup umožňuje včasné odhalení a řešení technických a bezpečnostních incidentů i mimo běžnou pracovní dobu.

ISO/IEC 27001:2022

Příloha A.5.30 - Dostupnost informací

- Vyžaduje implementaci opatření pro zajištění dostupnosti informací a zpracování informací.

Příloha A.8.9 - Monitorování

- Požaduje implementaci systémů pro kontinuální monitoring a zaznamenávání událostí.

Směrnice NIS2 (EU) 2022/2555

Článek 21 - Opatření k řízení rizik kybernetické bezpečnosti

2. Opatření uvedená v odstavci 1 zahrnují přinejmenším:

i) používání a vývoj postupů pro zachování dostupnosti služeb;

- Mobilní přístup představuje účinný postup pro zachování dostupnosti služeb díky možnosti rychlé reakce na incidenty.

2. Bezpečnostní důvody pro trvání na požadavku mobilní aplikace

2.1 Zvýšení reakční schopnosti při řešení kybernetických bezpečnostních incidentů

Mobilní přístup významně zvyšuje schopnost rychlé reakce na bezpečnostní incidenty:

- **Minimalizace MTTR (Mean Time To Respond)** - Zkrácení doby mezi detekcí incidentu a zahájením jeho řešení, což je kritický faktor při kybernetických útocích.
- **Nezávislost na fyzické lokaci** - Možnost reagovat na incidenty odkudkoliv a kdykoliv, což je klíčové v době, kdy kybernetické útoky jsou často načasovány na období mimo pracovní dobu.
- **Okamžitý přístup k diagnostickým nástrojům** - Možnost rychle analyzovat stav serveru a diagnostikovat povahu incidentu bez nutnosti přístupu k pracovní stanici.
- **Rychlé provádění kritických bezpečnostních zásahů** - Možnost okamžitého provedení kritických akcí jako je izolace serveru, restart služby nebo aplikace bezpečnostní záplaty.

2.2 Zvýšení efektivity bezpečnostního monitoringu

Mobilní aplikace poskytují efektivní nástroje pro kontinuální bezpečnostní monitoring:

- **Proaktivní notifikace o bezpečnostních událostech** - Přímé notifikace na mobilní zařízení o kritických bezpečnostních událostech.
- **Kontinuální monitoring kritických systémů** - Možnost průběžně sledovat stav kritických systémů i mimo standardní pracovní dobu.
- **Rychlá verifikace bezpečnostních alertů** - Možnost okamžitě ověřit legitimitu bezpečnostních alertů a minimalizovat false positives.
- **Zvýšená viditelnost bezpečnostních událostí** - Lepší přehled o bezpečnostních událostech napříč celou infrastrukturou.

2.3 Zajištění kontinuity provozu v případě kybernetických bezpečnostních incidentů

V případě kybernetického bezpečnostního incidentu poskytuje mobilní přístup kritické výhody:

- **Nezávislost na dostupnosti pracovních stanic** - Možnost řešit incidenty i v případě, že jsou pracovní stanice kompromitovány nebo nedostupné.
- **Záložní přístupový kanál** - Mobilní přístup může sloužit jako záložní přístupový kanál v případě narušení primárních přístupových cest.
- **Rychlá implementace krizových opatření** - Možnost rychle implementovat krizová opatření pro minimalizaci dopadů incidentu.
- **Podpora pro krizové řízení** - Efektivnější koordinace krizového řízení díky mobilnímu přístupu k informacím o stavu systémů.

2.4 Bezpečná aplikace aktualizací a bezpečnostních záplat

Mobilní aplikace umožňují bezpečnější a efektivnější nasazování aktualizací:

- **Rychlá reakce na zero-day zranitelnosti** - Možnost rychle aplikovat kritické bezpečnostní záplaty i mimo pracovní dobu.
- **Monitoring průběhu aktualizací** - Průběžné sledování stavu aplikace kritických aktualizací.
- **Okamžitá verifikace úspěšnosti aktualizace** - Možnost okamžitě ověřit úspěšnost aplikace bezpečnostních záplat.
- **Rychlý rollback při problémech** - V případě problémů s aktualizací možnost rychle provést rollback.

3. Technické zdůvodnění požadavku na mobilní aplikace

3.1 Moderní přístupy k správě infrastruktury založené na mobilním přístupu

Požadavek na mobilní přístup reflektuje moderní trendy v oblasti správy IT infrastruktury:

- **Integrace s cloudovými monitorovacími nástroji** - Mobilní aplikace jsou často úzce integrovány s cloudovými monitorovacími nástroji výrobce.
- **Jednotné prostředí pro správu heterogenní infrastruktury** - Možnost spravovat různorodou infrastrukturu prostřednictvím jednotného rozhraní.
- **Využití specifických funkcí mobilních zařízení** - Využití funkcí jako je biometrická autentizace, push notifikace nebo geolokace pro zvýšení bezpečnosti a komfortu správy.
- **Optimalizace pro efektivní mobilní správu** - Rozhraní optimalizované pro rychlé zásahy prostřednictvím dotykového ovládání.

3.2 Bezpečnostní funkce moderních mobilních aplikací pro správu serverů

Moderní mobilní aplikace pro správu serverů obsahují pokročilé bezpečnostní funkce:

- **Vícefaktorová autentizace** - Podpora pro vícefaktorovou autentizaci včetně biometrických metod.
- **End-to-end šifrování komunikace** - Zabezpečená komunikace mezi mobilním zařízením a spravovanými servery.
- **Časově omezené přístupové tokeny** - Využití časově omezených přístupových tokenů pro minimalizaci rizika zneužití.
- **Podrobné auditní logy** - Detailní záznamy o všech akcích provedených prostřednictvím mobilní aplikace.
- **Geofencing** - Možnost omezit přístup pouze z určitých geografických lokalit.

3.3 Výhody cloudového portálu výrobce pro správu serverů

Cloudový portál výrobce poskytuje významné výhody z hlediska bezpečnosti a efektivity správy:

- **Automatické aktualizace bezpečnostních definic** - Průběžné aktualizace bezpečnostních pravidel a definic.
- **Globální telemetrie a detekce hrozeb** - Využití globální telemetrie pro včasnou detekci nových hrozeb.
- **Proaktivní identifikace zranitelností** - Automatická identifikace zranitelností na základě globální databáze výrobce.
- **Integrace s bezpečnostními službami výrobce** - Využití specializovaných bezpečnostních služeb a expertízy výrobce.

4. Rozšířená dostupnost mobilních aplikací na trhu

4.1 Přehled výrobců nabízejících mobilní aplikace pro správu serverů

Zadavatel konstatuje, že požadavek na mobilní aplikace je splnitelný širokou škálou výrobců.

4.2 Dostupnost řešení třetích stran

Kromě nativních aplikací výrobců existují i řešení třetích stran, která umožňují mobilní přístup ke správě serverů:

- **Centralizované řešení správy infrastruktury** - Nástroje nabízejí mobilní aplikace pro monitoring a základní správu.
- **Specializované řešení pro mobilní přístup** - Řešení nabízejí zabezpečený mobilní přístup k serverům.

4.3 Open-source alternativy

Existují i open-source řešení, která mohou být integrována s nativními nástroji správy serverů.

5. Řešení potenciálních rizik spojených s mobilním přístupem

5.1 Minimalizace bezpečnostních rizik mobilního přístupu

Zadavatel si je vědom potenciálních rizik spojených s mobilním přístupem a bude vyžadovat implementaci následujících bezpečnostních opatření:

- **Striktní řízení přístupu** - Jasně definované role a oprávnění pro mobilní přístup.
- **Vícefaktorová autentizace** - Povinné použití vícefaktorové autentizace pro mobilní přístup.
- **Šifrování veškeré komunikace** - Zabezpečení veškeré komunikace mezi mobilním zařízením a serverovou infrastrukturou.
- **Detailní auditní logy** - Podrobné záznamy o všech akcích provedených prostřednictvím mobilního přístupu.

- **Mobile Device Management (MDM)** - Implementace řešení pro správu mobilních zařízení s přístupem k serverové infrastruktuře.
- **Automatické odhlášení** - Automatické ukončení relace po definované době nečinnosti.
- **Vzdálené vymazání dat** - Možnost vzdáleně vymazat přístupové údaje z mobilního zařízení v případě jeho ztráty nebo krádeže.

5.2 Integrace mobilního přístupu do celkové bezpečnostní architektury

Mobilní přístup bude integrován do celkové bezpečnostní architektury organizace:

- **Integrace s SIEM systémem** - Propojení auditních logů z mobilního přístupu do centrálního SIEM systému.
- **Synchronizace s IAM řešením** - Zajištění synchronizace s centrálním systémem správy identit a přístupů.
- **Soulad s bezpečnostními politikami** - Zajištění souladu mobilního přístupu s celkovými bezpečnostními politikami organizace.
- **Pravidelné bezpečnostní audity** - Zařazení mobilního přístupu do pravidelných bezpečnostních auditů.

6. Uvedení praktických scénářů využití mobilního přístupu

6.1 Konkrétní scénáře využití v prostředí školské instituce

- **Reakce na DDoS útok mimo pracovní dobu** - Mobilní přístup umožní rychlou reakci na DDoS útok zahájený například o víkendu nebo v noci.
- **Řešení kritické zranitelnosti během zkouškového období** - Možnost aplikovat kritické bezpečnostní záplaty během zkouškového období bez nutnosti fyzické přítomnosti na pracovišti.
- **Monitoring infrastruktury během důležitých akcí** - Kontinuální monitoring serverové infrastruktury během důležitých akcí (přijímací zkoušky, zápisy předmětů) i mimo kancelář.
- **Rychlá reakce na malware detekovaný v síti** - Možnost rychle izolovat infikované systémy i mimo pracovní dobu.
- **Ověření stavu infrastruktury po výpadku elektrické energie** - Rychlá kontrola stavu serverů po výpadku elektrické energie bez nutnosti cestovat na pracoviště.

6.2 Příklady reálných incidentů, kdy mobilní přístup byl kritický

- **Ransomware útoky o víkendu** - Mnoho ransomware útoků je načasováno na víkend, kdy je nižší pravděpodobnost okamžité reakce.
- **Zero-day zranitelnosti vyžadující okamžitou reakci** - Kritické zranitelnosti jako Log4Shell vyžadují okamžitou reakci nezávisle na denní době.
- **Phishing kampaně mimo pracovní dobu** - Phishingové kampaně často probíhají mimo standardní pracovní dobu, kdy je nižší ostražitost uživatelů.

7. Závěr

Zadavatel na základě výše uvedených důvodů trvá na požadavku přístupu do cloudového portálu výrobce serverů a ovládání grafické konzole pro správu a monitorování serverů také přes mobilní aplikace dostupné pro iOS a Android. Tento požadavek přímo přispívá k naplnění cílů zakázky v oblasti zajištění kybernetické bezpečnosti, zejména rychlé reakce na bezpečnostní incidenty a minimalizace doby nedostupnosti služeb.

Zadavatel konstatuje, že tento požadavek je splnitelný širokou škálou výrobců na trhu a nepředstavuje nepřiměřené omezení hospodářské soutěže. Potenciální bezpečnostní rizika spojená s mobilním přístupem budou řešena implementací adekvátních bezpečnostních opatření v souladu s nejlepšími praktikami a standardy v oblasti kybernetické bezpečnosti.

Pro úplnost zadavatel uvádí, že v případě, že dodavatel má obavy o schopnost splnit tento požadavek, může v souladu s § 89 odst. 6 ZZVZ nabídnout řešení, které je technicky rovnocenné nebo které představuje vyšší kvalitu než požadovaná specifikace.

Dotaz č. 4:

Požadavek na rozhraní backup serveru

Požadavek na 2 VGA rozhraní (1 vpředu, 1 vzadu) je dle našeho názoru nepřiměřený a de facto odpovídá technickému řešení konkrétních výrobců (např. Dell). Žádáme o vysvětlení, jaký konkrétní bezpečnostní benefit má požadavek na 2 ks VGA rozhraní přinést příp. revizi počtu na obvyklou a odůvodnitelnou hodnotu 1 ks VGA rozhraní vzadu. U virtualizačních serverů požadavek na VGA rozhraní není uveden.

Odpověď na dotaz č. 4:

Zadavatel trvá na požadavku podpory multitenantního přístupu a možnosti delegování přístupu k samostatným tenantům u switchů a aktivních prvků, a to z následujících důvodů souvisejících s kybernetickou bezpečností školské instituce:

1. Princip nejnižších oprávnění (Principle of Least Privilege)
Podpora multitenantního přístupu je klíčovým nástrojem pro implementaci principu nejnižších oprávnění, který je základním požadavkem moderní kybernetické bezpečnosti a je explicitně vyžadován v § 17 odst. 3 písm. b) Vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb. ("řízení přístupu k síťovým službám"). Tento princip vyžaduje, aby různé role v organizaci měly přístup pouze k těm částem infrastruktury, které nutně potřebují ke své práci.
V prostředí školské instituce to znamená:

- IT správci jednotlivých oddělení/fakult potřebují spravovat pouze síťové segmenty příslušné jejich zodpovědnosti
- Externí dodavatelé služeb (např. správci specializovaných učeben) potřebují přístup pouze k vyhrazeným segmentům sítě
- Dočasní správci (např. při projektových aktivitách) potřebují časově omezený přístup k vybraným částem infrastruktury

2. Ochrana před insider threats a omezení dopadů kompromitace
Delegování přístupu k samostatným tenantům významně snižuje riziko tzv. "insider threats" - úmyslných či neúmyslných bezpečnostních incidentů způsobených oprávněnými uživateli. Tato schopnost je v souladu s požadavky § 18 Vyhlášky o kybernetické bezpečnosti na "nástroje pro detekci kybernetických bezpečnostních událostí" a § 20 na "zaznamenávání událostí informačního a komunikačního systému".
Konkrétní přínosy pro kybernetickou bezpečnost:

- Omezení škod při kompromitaci účtu správce - útočník získá přístup pouze k omezenému segmentu sítě
- Snazší detekce anomálií - systém může identifikovat neobvyklé chování v rámci jednotlivých tenantů
- Přesnější identifikace původce bezpečnostního incidentu díky granulárnímu logování přístupů
- Efektivnější incident response - možnost izolovat pouze zasažené tenanty při bezpečnostním incidentu

3. Soulad s požadavky na segmentaci sítě a mikrosegmentaci
Multitenantní přístup je technologickým předpokladem pro účinnou implementaci mikrosegmentace sítě, která je vyžadována v § 17 odst. 3 písm. d) Vyhlášky o kybernetické bezpečnosti ("provádění segmentace sítě"). Ve školním prostředí je nezbytné vytvářet oddělené segmenty pro:

- Administrativní síť s citlivými osobními údaji studentů a zaměstnanců
- Studentské sítě s různými úrovněmi přístupu (běžné učebny, specializované laboratoře)
- IoT zařízení (tiskárny, projektory, zabezpečovací systémy)
- Výzkumné projekty s různými bezpečnostními požadavky

Každý segment vyžaduje specifická bezpečnostní pravidla a oddělené správcovské role, což je možné efektivně realizovat pouze s podporou multitenantního přístupu.
4. Auditovatelnost a transparentnost správy
Podpora multitenantu s delegováním přístupu zajišťuje kompletní auditovatelnost prováděných změn a přístupů, což je nezbytné pro splnění požadavků § 20 Vyhlášky o kybernetické bezpečnosti na "zaznamenávání událostí informačního a komunikačního systému" a § 23 na "sběr a vyhodnocování kybernetických bezpečnostních událostí".
Pro školské zařízení to znamená:

- Možnost prokázat, kdo, kdy a jaké změny v síťové infrastruktuře provedl
- Schopnost detekovat neoprávněné změny konfigurace napříč celou infrastrukturou
- Přesná evidence přístupů v souladu s požadavky GDPR na zpracování osobních údajů
- Podklady pro pravidelné bezpečnostní audity vyžadované Zákonem o kybernetické bezpečnosti

5. Soulad s doporučeními NÚKIB a mezinárodními standardy
Požadavek na multitenantní přístup je v souladu s:

- Doporučením NÚKIB pro segmentaci sítí (dokument "Bezpečnostní doporučení pro administrátory")
- Rámcem NIST Cybersecurity Framework (funkce ID.AM, PR.AC, PR.PT, DE.CM)
- Standardem ISO/IEC 27001:2022, příloha A.5 (Organizační opatření) a A.8 (Řízení přístupu)
- Požadavky směrnice NIS2 (EU) 2022/2555, článek 21 na "řízení rizik kybernetické bezpečnosti"

6. Specifické bezpečnostní scénáře pro školní prostředí
Multitenantní přístup umožňuje efektivní řešení následujících bezpečnostních scénářů specifických pro školní prostředí:
a) **Zabezpečení speciálních akcí** - Při organizaci akcí jako jsou přijímací zkoušky, státní zkoušky nebo certifikační testování je nutné dočasně vytvořit izolované síťové prostředí s oddělenou správou.
b) **Výzkumné projekty s externími partnery** - Při spolupráci s externími institucemi na výzkumných projektech je nezbytné poskytnout omezenou míru přístupu externím partnerům bez ohrožení zbytku infrastruktury.

c) **Studentské projekty** - Možnost vytvářet bezpečné "pískoviště" pro studentské síťové projekty s omezeným dohledem vyučujících bez rizika pro produkční síť.
d) **Odolnost vůči ransomware útokům** - V případě ransomware útoku, který je jednou z nejčastějších hrozeb pro vzdělávací instituce, umožňuje multitenantní architektura rychlou izolaci zasažených částí sítě bez nutnosti vypnutí celé infrastruktury.
Závěr
Požadavek na podporu multitenantního přístupu a možnosti delegování přístupu k samostatným tenantům u switchů a aktivních prvků je přímo spjat s cílem zakázky zajistit kybernetickou bezpečnost školského zařízení. Tento požadavek vychází z platné legislativy v oblasti kybernetické bezpečnosti, doporučení NÚKIB a mezinárodních standardů, a jeho implementace je nezbytná pro efektivní řízení přístupu, segmentaci sítě, auditovatelnost a ochranu proti moderním kybernetickým hrozbám.
Zadavatel proto na tomto požadavku trvá jako na základním prvku zajištění kybernetické bezpečnosti školské instituce.

Dotaz č. 5:
Požadavky omezující soutěž u položky WiFi AP a u položky NAC
Omezení cloudových platforem pouze na služby AWS/Google Cloud/Microsoft Azure: "Služba SaaS provozovaná v datových centrech v rámci EU na platformách AWS/Google Cloud/Microsoft Azure s garantovanou dostupností."
Specifikace „Služba SaaS provozovaná na platformách AWS/Google Cloud/Microsoft Azure“ diskriminuje dodavatele využívající privátní datová centra.
Z naší zkušenosti dává smysl doplnění možnosti využití privátního datového centra výrobce s garantovanou dostupností – tzn. sjednocení daného požadavku s požadavkem zadavatele uvedeným u položek core switche a u aktivních prvků: "Služba provozovaná v datových centrech v rámci EU na platformách AWS/Google Cloud/Microsoft Azure, případně v privátním datovém centru výrobce s garantovanou dostupností."

Odpověď na dotaz č. 5:
Zadavatel trvá na požadavku, aby služba SaaS byla provozována výhradně v datových centrech v rámci EU na platformách AWS/Google Cloud/Microsoft Azure s garantovanou dostupností. Tento požadavek je klíčový pro zajištění kybernetické bezpečnosti, splnění legislativních požadavků a zajištění dlouhodobé udržitelnosti řešení. Níže uvedené zdůvodnění objasňuje, proč je v tomto specifickém případě nezbytné trvat na uvedených veřejných cloudových platformách a proč se tento požadavek liší od požadavků na infrastrukturu pro core switche a další aktivní prvky.
1. Legislativní opory požadavku
Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
§ 4 odst. 1 - "Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru."

- Využití certifikovaných veřejných cloudových platforem významně přispívá k zajištění bezpečnosti informací a dostupnosti služeb díky jejich robustním bezpečnostním mechanismům a globální infrastruktuře.

§ 4 odst. 2 - "Orgány a osoby... jsou povinny zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti..."

- Vyžadované cloudové platformy poskytují komplexní bezpečnostní opatření, která jsou nezbytná pro zajištění kybernetické bezpečnosti informačních systémů.

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních
§ 11 - Řízení rizik
(1) Povinná osoba v rámci řízení rizik
a) stanoví metodiku pro identifikaci, hodnocení a zvládání rizik,
c) při hodnocení rizik posuzuje možné dopady na informační a komunikační systém, zejména dostupnost, důvěrnost a integritu,

- Veřejné cloudové platformy AWS, Google Cloud a Microsoft Azure poskytují robustní nástroje pro řízení rizik, monitoring a zajištění dostupnosti, důvěrnosti a integrity dat.

§ 16 - Bezpečnost provozu
(3) Povinná osoba v rámci bezpečnosti provozu informačního a komunikačního systému dále zajistí
a) detekci kybernetických bezpečnostních událostí,

b) sběr a vyhodnocení kybernetických bezpečnostních událostí,

- Vyžadované cloudové platformy poskytují pokročilé nástroje pro detekci, sběr a vyhodnocení bezpečnostních událostí.

Nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR)

Článek 32 - Bezpečnost zpracování

1. S přihlédnutím ke stavu techniky... správce a zpracovatel provedou vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku...

- Vyžadované cloudové platformy poskytují certifikovaná technická a organizační opatření, která odpovídají aktuálnímu stavu techniky a umožňují soulad s požadavky GDPR.

Směrnice NIS2 (EU) 2022/2555

Článek 21 - Opatření k řízení rizik kybernetické bezpečnosti

2. Opatření uvedená v odstavci 1 zahrnují přinejmenším:

b) postupy pro obnovení podnikání a kontinuity, jako je správa záloh a obnova po havárii, a řízení krizí;

- AWS, Google Cloud a Microsoft Azure poskytují komprehensivní nástroje pro zajištění kontinuity podnikání a obnovu po havárii, které často převyšují možnosti privátních datových center.

2. Bezpečnostní důvody pro trvání na požadavku veřejných cloudových platforem

2.1 Certifikace a soulad s mezinárodními bezpečnostními standardy

Veřejné cloudové platformy AWS, Google Cloud a Microsoft Azure disponují rozsáhlými a mezinárodně uznávanými certifikacemi:

- **Komplexní bezpečnostní certifikace** - Všechny tři vyžadované platformy mají certifikace ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC 3, PCI DSS, GDPR a další.
- **Certifikace pro státní správu** - Platformy mají specifické certifikace pro státní správu jako FedRAMP v USA nebo ENISA Cybersecurity Certification Scheme v EU.
- **Oborové certifikace** - Disponují certifikacemi relevantními pro vzdělávací sektor a zpracování citlivých dat.
- **Standardizované audit logy** - Poskytují standardizované a nezávisle auditovatelné logy splňující požadavky regulačních orgánů.

2.2 Pokročilé bezpečnostní funkce a ochrana proti kybernetickým útokům

Vyžadované cloudové platformy nabízejí pokročilé bezpečnostní funkce, které často nejsou dostupné v privátních datových centrech:

- **Globální DDoS ochrana** - Robustní ochrana proti DDoS útokům s kapacitou v řádu Tbps, kterou privátní datová centra obvykle nemohou dosáhnout.
- **Pokročilá detekce a prevence průniků** - Využití umělé inteligence a strojového učení pro detekci a prevenci sofistikovaných útoků.
- **Automatizované bezpečnostní patche** - Automatické nasazování bezpečnostních záplat bez výpadků služeb.
- **Zero-Trust architektura** - Implementace nejmodernějších zero-trust bezpečnostních modelů.
- **Globální monitoring hrozeb** - Využití globální telemetrie a rozpoznávání vzorců útoků napříč miliony zákazníků.

2.3 Garance dostupnosti a kontinuity služeb

Veřejné cloudové platformy poskytují úroveň dostupnosti, kterou privátní datová centra obvykle nemohou garantovat:

- **Geografická redundance v rámci EU** - Možnost automatické replikace dat a služeb mezi různými regiony v rámci EU.
- **Smluvně garantovaná dostupnost (SLA)** - Jasně definované SLA s finančními kompenzacemi při nedodržení.
- **Transparentní monitoring výpadků** - Veřejně dostupný status stránky a transparentní komunikace o výpadcích.
- **Automatizované disaster recovery** - Pokročilé nástroje pro automatizované zotavení po havárii.
- **Stabilní a predikovatelná latence** - Optimalizovaná síťová infrastruktura zajišťující stabilní latenci.

3. Technologické důvody pro trvání na požadavku veřejných cloudových platforem

3.1 Standardizované API a integrace

Vyžadované cloudové platformy poskytují standardizovaná API, která jsou klíčová pro integraci s dalšími systémy zadavatele:

- **Standardizovaná a dobře dokumentovaná API** - AWS, Google Cloud a Microsoft Azure poskytují komplexní, stabilní a dobře dokumentovaná API.

- **Široká podpora vývojářských nástrojů** - Rozsáhlá podpora vývojářských nástrojů, knihoven a frameworků.
- **Interoperabilita mezi systémy** - Snazší integrace s ostatními systémy díky standardizovaným rozhraním.
- **Ekosystém třetích stran** - Rozsáhlý ekosystém řešení třetích stran certifikovaných pro tyto platformy.

3.2 Škálovatelnost a flexibilita

Veřejné cloudové platformy nabízejí bezkonkurenční škálovatelnost a flexibilitu:

- **Automatické škálování** - Schopnost automaticky škálovat zdroje podle aktuálního zatížení.
- **Globální škálovatelnost** - Možnost globálního škálování při zachování lokálního zpracování dat v EU.
- **Flexibilní alokace zdrojů** - Možnost dynamicky přidělovat a uvolňovat výpočetní zdroje.
- **Adaptace na špičkové zatížení** - Schopnost automaticky zvládnout špičkové zatížení (např. během přijímacích zkoušek nebo zápisů).

3.3 Technologická inovace a dlouhodobá udržitelnost

Vyžadované platformy zajišťují přístup k nejnovějším technologiím a dlouhodobou udržitelnost:

- **Kontinuální technologická inovace** - Pravidelné zavádění nových služeb a technologických vylepšení.
- **Podpora moderních architektur** - Rozsáhlá podpora pro serverless, kontejnery, mikroslužby a další moderní architektury.
- **Dlouhodobá strategická vize** - Jasné roadmapy a dlouhodobé vize vývoje platforem.
- **Investice do výzkumu a vývoje** - Masivní investice do R&D, které zajišťují technologický náskok.

4. Právní a compliance aspekty

4.1 GDPR a lokalizace dat v EU

Požadavek na datová centra v rámci EU zajišťuje soulad s GDPR a dalšími evropskými regulacemi:

- **Garance umístění dat v EU** - Všechny tři platformy umožňují garantovat umístění dat výhradně v EU.
- **Transparentní zpracování dat** - Jasně definované podmínky zpracování dat v souladu s GDPR.
- **GDPR-ready infrastruktura** - Infrastruktura navržená s ohledem na požadavky GDPR.
- **Standardní smluvní doložky (SCC)** - Implementace standardních smluvních doložek pro přenos dat.

4.2 Compliance s požadavky na zpracování osobních údajů

Veřejné cloudové platformy poskytují robustní nástroje pro compliance:

- **DPA (Data Processing Addendum)** - Standardizované dodatky ke zpracování osobních údajů.
- **Nástroje pro řízení compliance** - Pokročilé nástroje pro monitoring a reporting compliance.
- **Audit trail a nezměnitelné logy** - Robustní systémy pro vedení auditních záznamů a nezměnitelných logů.
- **Automatizovaná klasifikace dat** - Nástroje pro automatickou klasifikaci dat podle citlivosti.

4.3 Transparentnost a právní jistota

Vyžadované platformy poskytují vysokou míru transparentnosti a právní jistoty:

- **Standardizované smluvní podmínky** - Jasně definované a veřejně dostupné smluvní podmínky.
- **Transparentní cenová politika** - Veřejně dostupné ceníky a kalkulátory nákladů.
- **Přehledné podmínky ukončení služby** - Jasně definované podmínky pro export dat a ukončení služby.
- **Nezávislé právní audity** - Platformy jsou pravidelně podrobovány nezávislým právním auditům.

5. Zdůvodnění rozdílu v přístupu oproti jiným položkám zakázky

5.1 Odlišná povaha služeb SaaS oproti infrastrukturním službám

Požadavek na veřejné cloudové platformy pro služby SaaS se liší od požadavků na infrastrukturu pro core switche a jiné aktivní prvky z následujících důvodů:

- **Přímo spravovaná data vs. monitorovací metadata** - SaaS služby přímo zpracovávají a ukládají citlivá data organizace, zatímco monitorovací služby pro aktivní prvky typicky pracují pouze s metadaty.
- **Různá úroveň kritičnosti** - SaaS služby často představují kritičtější komponenty z hlediska bezpečnosti a dostupnosti než monitorovací služby pro aktivní prvky.
- **Odlišné požadavky na integraci** - SaaS služby vyžadují hlubší integraci s ostatními systémy organizace než monitorovací služby pro aktivní prvky.
- **Rozdílné požadavky na compliance** - SaaS služby podléhají přísnějším regulačním požadavkům vzhledem k povaze zpracovávaných dat.

5.2 Specifické bezpečnostní požadavky pro SaaS služby

SaaS služby vyžadují specifické bezpečnostní záruky, které jsou lépe zajištěny veřejnými cloudovými platformami:

- **Víceúrovňová ochrana dat** - SaaS služby vyžadují komplexnější přístup k ochraně dat v klidu i za pohybu.
- **Pokročilá autentizace a autorizace** - Potřeba pokročilých systémů pro správu identit a přístupů.

- **Kontinuální bezpečnostní monitoring** - Potřeba nepřetržitého monitoringu bezpečnostních událostí.
- **Certifikovaná bezpečnostní infrastruktura** - Požadavek na certifikovanou infrastrukturu splňující přísné bezpečnostní standardy.

5.3 Technické rozdíly mezi SaaS a monitoringem aktivních prvků

Z technického hlediska existují zásadní rozdíly mezi SaaS službami a monitoringem aktivních prvků:

- **Architektonické rozdíly** - SaaS služby vyžadují komplexnější architekturu než monitorovací služby pro aktivní prvky.
- **Rozdílné nároky na výpočetní zdroje** - SaaS služby mají typicky vyšší a dynamičtější nároky na výpočetní zdroje.
- **Různé požadavky na latenci** - SaaS služby často vyžadují nižší a stabilnější latenci pro zajištění uživatelského komfortu.
- **Odlišné nároky na zálohování a DR** - SaaS služby vyžadují sofistikovanější přístupy k zálohování a disaster recovery.

6. Analýza tržní dostupnosti požadovaného řešení

6.1 Dostupnost SaaS řešení na vyžadovaných platformách

Zadavatel provedl průzkum trhu a zjistil, že:

- **Široká nabídka řešení** - Na trhu existuje dostatečně široká nabídka SaaS řešení provozovaných na vyžadovaných platformách.
- **Konkurenční prostředí** - Požadavek na AWS, Google Cloud nebo Microsoft Azure umožňuje účast dostatečného počtu potenciálních dodavatelů.
- **Různé cenové kategorie** - Na trhu jsou dostupná řešení v různých cenových kategoriích, od ekonomických po prémiová.
- **Rozmanitost funkcionalit** - Dostupná řešení pokrývají širokou škálu funkcionalit a specializací.

6.2 Srovnání s privátními datovými centry

Analýza privátních datových center ve srovnání s vyžadovanými veřejnými cloudovými platformami ukazuje:

- **Bezpečnostní certifikace** - Privátní datová centra výrobců typicky nedisponují tak širokým spektrem bezpečnostních certifikací.
- **Geografická redundance** - Privátní datová centra obvykle neposkytují tak robustní geografickou redundanci v rámci EU.
- **Garantovaná dostupnost** - SLA v privátních datových centrech často nedosahují úrovně poskytované veřejnými cloudovými platformami.
- **Transparentnost bezpečnostních praktik** - Privátní datová centra obvykle neposkytují stejnou úroveň transparentnosti ohledně bezpečnostních praktik.

7. Závěr

Zadavatel na základě výše uvedených důvodů trvá na požadavku, aby služba SaaS byla provozována výhradně v datových centrech v rámci EU na platformách AWS/Google Cloud/Microsoft Azure s garantovanou dostupností. Tento požadavek je v souladu s právními předpisy, zajišťuje požadovanou úroveň kybernetické bezpečnosti a garantuje dlouhodobou udržitelnost řešení.

Zadavatel konstatuje, že tento požadavek nepředstavuje nepřiměřené omezení hospodářské soutěže, neboť na trhu existuje dostatečné množství potenciálních dodavatelů, kteří jsou schopni tento požadavek splnit. Požadavek je zároveň přiměřený ve vztahu k předmětu zakázky a její předpokládané hodnotě.

Odlišný přístup k požadavkům na infrastrukturu pro core switche a další aktivní prvky je odůvodněn rozdílnou povahou těchto služeb, nižší úrovní kritičnosti a odlišnými požadavky na compliance a integraci.

Zadavatel tedy odmítá připomínku dodavatele jako neopodstatněnou a trvá na původním znění požadavku.

Dotaz č. 6:

Požadavek na MACsec na portech zařízení u firewallu.

Požadavek na MACsec u firewallů je dle běžných standardů nadbytečný, protože šifrování provozu se typicky řeší na úrovni switchů. Žádáme o odstranění tohoto požadavku nebo vysvětlení, proč je nezbytný právě u firewallů.

Odpověď na dotaz č. 6:

Zadavatel trvá na požadavku podpory MACsec (IEEE 802.1AE) u firewallů, a to z následujících důvodů souvisejících s kybernetickou bezpečností školské instituce:

1. Legislativní opory požadavku

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

§ 4 odst. 1 - Zákon definuje bezpečnostní opatření jako "souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru."

- Implementace MACsec na firewallech představuje dodatečnou vrstvu ochrany, která zvyšuje celkovou bezpečnost sítě.

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních

§ 17 - Bezpečnost komunikačních sítí

(3) Povinná osoba v rámci ochrany integrity komunikačních sítí c) chrání vzdálený přístup pomocí kryptografie,

- MACsec poskytuje silné kryptografické zabezpečení na linkové vrstvě mezi kritickými síťovými prvky.

§ 26 - Kryptografické prostředky

(1) Povinná osoba používá kryptografické prostředky, které zajistí ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a zajistí požadovanou úroveň dostupnosti. (3) Povinná osoba pro kryptografickou ochranu v informačním a komunikačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury nebo významném informačním systému používá pouze nástroje, které a) používají certifikované kryptografické prostředky, nebo b) používají doporučené kryptografické algoritmy.

- MACsec implementuje doporučené kryptografické algoritmy a poskytuje certifikovanou ochranu na linkové vrstvě.

ISO/IEC 27001:2022

Příloha A.5.14 - Kryptografie

Kryptografické mechanismy musí být aplikovány v souladu s formálními zásadami, postupy a metodami.

- MACsec představuje standardizovaný kryptografický mechanismus (IEEE 802.1AE), který je v souladu s formálními zásadami kybernetické bezpečnosti.

Směrnice NIS2 (EU) 2022/2555

Článek 21 - Opatření k řízení rizik kybernetické bezpečnosti

2. Opatření uvedená v odstavci 1 zahrnují přinejmenším: c) bezpečnost komunikace a přenosu dat;

- MACsec na firewallech přímo přispívá k zajištění bezpečnosti komunikace a přenosu dat v souladu s požadavky směrnice NIS2.

2. Bezpečnostní důvody pro implementaci MACsec na firewallech

2.1 Princip hloubkové obrany (Defense in Depth)

Implementace MACsec na firewallech, i když je tato technologie již nasazena na switchích, vychází z principu hloubkové obrany, který je jedním ze základních pilířů kybernetické bezpečnosti. Tento princip vyžaduje nasazení více nezávislých bezpečnostních mechanismů pro ochranu kritických systémů:

- **Nezávislé bezpečnostní vrstvy** - V případě kompromitace switchů nebo jejich MACsec implementace zůstává zachována ochrana na úrovni firewallů.
- **Eliminace single point of failure** - Zabezpečení není závislé pouze na jedné vrstvě infrastruktury.
- **Soulad s doporučeními NÚKIB** - Národní úřad pro kybernetickou a informační bezpečnost doporučuje implementaci principu hloubkové obrany pro kritickou infrastrukturu.

2.2 Ochrana hraničních bodů sítě a DMZ

Firewall představuje hraniční bod sítě, kde dochází k propojení různých bezpečnostních zón:

- **Zabezpečení spojení mezi bezpečnostními zónami** - MACsec zajišťuje, že data přenášená mezi různými bezpečnostními zónami (např. mezi interní sítí a DMZ) jsou chráněna na linkové vrstvě.
- **Ochrana proti MITM útokům v kritických bodech** - Hraniční body sítě jsou primárním cílem útočníků pro implementaci Man-in-the-Middle útoků.
- **Verifikace integrity provozu** - MACsec poskytuje funkce pro zajištění integrity dat, což je klíčové při přenosu mezi bezpečnostními zónami.

2.3 Zabezpečení horizontálního síťového provozu (East-West Traffic)

V moderní síťové architektuře značná část provozu probíhá horizontálně mezi servery v různých částech sítě (tzv. East-West Traffic):

- **Zabezpečení komunikace mezi segmenty** - Firewall často řídí komunikaci mezi různými segmenty sítě, a MACsec zajišťuje ochranu této komunikace.
- **Ochrana kritických datových toků** - MACsec chrání horizontální provoz mezi kritickými servery a službami (např. databázové servery, autentizační služby).
- **Detekce manipulace s provozem** - MACsec umožňuje detekovat jakoukoliv manipulaci s datovými toky mezi segmenty sítě.

2.4 Ochrana proti pokročilým hrozbám a APT útokům

Pokročilé perzistentní hrozby (APT) často využívají sofistikované metody k odposlouchávání síťového provozu:

- **Prevence skrytého odposlouchávání** - MACsec na firewallech znemožňuje odposlouchávání provozu i v případě, že útočník získal přístup k síti mezi firewallem a switchem.
- **Ochrana proti protokolovým analyzátorům** - MACsec zabraňuje analýze síťového provozu, která je často součástí první fáze APT útoku.
- **Mitigace rizik spojených s insidery** - Ochrana proti hrozbám ze strany privilegovaných uživatelů, kteří mají přístup k síťové infrastruktuře.

3. Specifické bezpečnostní scénáře pro školní prostředí

3.1 Ochrana citlivých výzkumných dat a duševního vlastnictví

Školské instituce, zejména vysoké školy, často pracují s cennými výzkumnými daty a duševním vlastnictvím:

- **Zabezpečení přenosu výzkumných dat** - MACsec na firewallech zajišťuje dodatečnou vrstvu ochrany při komunikaci mezi výzkumnými pracovišti a externími partnery.
- **Ochrana při mezinárodní spolupráci** - Zvýšená bezpečnost pro mezinárodní výzkumné projekty, které jsou častým cílem APT útoků.
- **Soulad s požadavky grantových agentur** - Řada grantových agentur vyžaduje implementaci pokročilých bezpečnostních mechanismů pro ochranu výzkumných dat.

3.2 Zabezpečení systémů pro online testování a hodnocení

Systémy pro online testování a hodnocení jsou kritické pro zajištění integrity vzdělávacího procesu:

- **Ochrana proti manipulaci s výsledky** - MACsec poskytuje dodatečnou vrstvu zabezpečení proti pokusům o manipulaci s výsledky testů nebo zkoušek.
- **Zabezpečení přenosu testových materiálů** - Zajištění důvěrnosti a integrity při přenosu testových materiálů a odpovědí.
- **Auditovatelnost přenosu dat** - MACsec v kombinaci s dalšími bezpečnostními mechanismy umožňuje auditovat integritu přenosu dat souvisejících s hodnocením.

3.3 Bezpečnost při propojení s partnerskými institucemi a externími vzdělávacími platformami

Moderní vzdělávací instituce jsou propojeny s řadou externích systémů a platforem:

- **Zabezpečení propojení s partnerskými školami** - MACsec na firewallech zajišťuje bezpečnou komunikaci při sdílení vzdělávacích materiálů a dat s partnerskými institucemi.
- **Ochrana propojení s cloudovými vzdělávacími platformami** - Dodatečná vrstva zabezpečení při komunikaci s externími vzdělávacími platformami.
- **Bezpečnost při napojení na akademické sítě** - Zvýšená ochrana při propojení s akademickými sítěmi jako CESNET, GÉANT apod.

4. Technická zdůvodnění požadavku MACsec na firewallech

4.1 Rozdílné bezpečnostní požadavky na různé síťové prvky

Implementace MACsec pouze na switchích nemusí poskytnout dostatečnou ochranu z několika důvodů:

- **Rozdílné bezpečnostní zóny** - Firewall často spojuje sítě s různými bezpečnostními požadavky, kde je žádoucí mít nezávislé zabezpečení.
- **Heterogenní síťové prostředí** - V reálném prostředí nemusí všechny switche podporovat MACsec nebo mohou mít různé implementace.
- **Granulární bezpečnostní politiky** - MACsec na firewallech umožňuje aplikovat specifické bezpečnostní politiky pro různé typy provozu.

4.2 Ochrana proti insider threat v síťové infrastruktuře

Interní hrozby představují významné riziko pro školní sítě:

- **Oddělení správcovských rolí** - MACsec na firewallech umožňuje implementovat princip oddělení povinností mezi správci switchů a firewallů.
- **Prevence neoprávněného odposlouchávání** - Ochrana proti neoprávněnému odposlouchávání ze strany oprávněných správců switchů.
- **Auditovatelnost přístupu k síťovému provozu** - MACsec přispívá k lepší auditovatelnosti přístupu k síťovému provozu.

4.3 Odolnost proti selhání nebo kompromitaci jednotlivých prvků

Redundantní implementace MACsec zvyšuje odolnost sítě:

- **Ochrana v případě selhání nebo obejití MACsec na switchi** - Pokud dojde k chybě konfigurace nebo objevení zranitelnosti v implementaci MACsec na switchi, firewall poskytuje záložní ochranu.
- **Obrana proti zero-day útokům** - Různé implementace MACsec mohou být odolné vůči různým typům zranitelností.
- **Soulad s principem N+1 redundance** - Implementace MACsec na více vrstvách síťové infrastruktury zajišťuje redundanci bezpečnostních mechanismů.

5. Závěr

Požadavek na podporu MACsec u firewallů je plně opodstatněný z hlediska zajištění kybernetické bezpečnosti školské instituce a má přímou oporu v Zákoně o kybernetické bezpečnosti, Vyhlášce č. 82/2018 Sb., standardu ISO/IEC 27001:2022 a směrnici NIS2. Tento požadavek implementuje princip hloubkové obrany, zvyšuje ochranu proti pokročilým hrozbám a reflektuje specifické bezpečnostní potřeby vzdělávacího sektoru.
I když je běžnou praxí implementovat MACsec primárně na úrovni switchů, jeho implementace na firewallech poskytuje dodatečnou vrstvu zabezpečení, která je v kontextu ochrany kritických dat a systémů vzdělávací instituce zcela opodstatněná. Odstranění tohoto požadavku by vedlo ke snížení celkové úrovně zabezpečení sítě a bylo by v rozporu s principy moderní kybernetické bezpečnosti.
Zadavatel proto trvá na zachování požadavku podpory MACsec u firewallů jako důležitého prvku své strategie kybernetické bezpečnosti.

Dotaz č. 7:
Požadavek u firewallů na min. 400 logických bezpečnostních zón, mezi kterými lze konfigurovat bezpečnostní politiky.
Požadavek na 400 zón je pro školské zařízení dané velikosti nepřiměřený a odporuje principu proporcionality (§ 6 ZZVZ). Žádáme o vysvětlení, jaký konkrétní bezpečnostní benefit má toto číslo přinést příp. revizi počtu na technicky odůvodnitelnou hodnotu. Z naší zkušenosti a Best Practice by pro dané řešení plně dostačovalo max. 100 logických bezpečnostních zón.

Odpověď na dotaz č. 7:
Zadavatel trvá na požadavku podpory 400 bezpečnostních zón, a to z důvodů souvisejících s kybernetickou bezpečností školské instituce a souladu s aktuálními bezpečnostními požadavky. Tento požadavek je přiměřený vzhledem k charakteru, rozsahu a bezpečnostním potřebám školského zařízení a jeho dlouhodobému rozvoji.
1. Legislativní opory požadavku
Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
§ 4 odst. 1 - "Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru."

- Vysoký počet bezpečnostních zón přispívá k zajištění bezpečnosti informací implementací principu mikrosegmentace.

§ 5 odst. 1 - "Povinné osoby jsou povinny v rozsahu nezbytném pro zajištění kybernetické bezpečnosti zavést a provádět bezpečnostní opatření pro informační systém nebo službu a vést o nich dokumentaci."

- Implementace granulární segmentace sítě patří mezi základní bezpečnostní opatření.

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních
§ 17 - Bezpečnost komunikačních sítí
(3) Povinná osoba v rámci ochrany integrity komunikačních sítí
d) provádí segmentaci sítě,

- Vyhláška explicitně požaduje segmentaci sítě, přičemž větší počet bezpečnostních zón umožňuje jemnější a efektivnější segmentaci.

§ 19 - Řízení přístupu
(1) Povinná osoba používá nástroje pro řízení přístupu, které
d) zajistí ověření identity uživatelů před zahájením aktivit v informačním a komunikačním systému,
e) zajistí řízení přístupu k jednotlivým technickým aktivům a jejich funkcím,

- Větší počet bezpečnostních zón umožňuje jemnější řízení přístupu na úrovni funkcí a aktiv.

ISO/IEC 27001:2022
Příloha A.8 - Řízení přístupu

- Zahrnuje požadavky na segmentaci sítí a implementaci principu nejnižších oprávnění.

Směrnice NIS2 (EU) 2022/2555
Článek 21 - Opatření k řízení rizik kybernetické bezpečnosti
2. Opatření uvedená v odstavci 1 zahrnují přinejmenším:
f) zásady kontroly přístupu, řízení přístupu a autentizace;

- Vysoký počet bezpečnostních zón podporuje implementaci zásad kontroly a řízení přístupu.

2. Bezpečnostní důvody pro požadavek 400 bezpečnostních zón
2.1 Implementace mikrosegmentace v souladu s Zero Trust architekturou
Moderní přístup k zabezpečení sítí je založen na konceptu Zero Trust, který vyžaduje jemnou mikrosegmentaci:

- **Segmentace na úrovni aplikací** - Každá kritická aplikace by měla mít svou vlastní bezpečnostní zónu

- **Segmentace na úrovni služeb** - Jednotlivé služby v rámci aplikace vyžadují různé bezpečnostní politiky
- **Izolace dle citlivosti dat** - Různé úrovně citlivosti dat vyžadují oddělené bezpečnostní zóny
- **Dynamické přidělování zón** - Zero Trust architektura vyžaduje dynamické přidělování bezpečnostních zón na základě kontextu

Doporučení NÚKIB pro implementaci Zero Trust vyžaduje granulární segmentaci sítě, která se neomezuje pouze na tradiční perimetrické rozdělení, ale segmentuje síť na úrovni jednotlivých služeb a aplikací.

2.2 Omezení rozsahu dopadu bezpečnostních incidentů

Jemná segmentace prostřednictvím většího počtu bezpečnostních zón významně omezuje potenciální dopad bezpečnostních incidentů:

- **Omezení laterálního pohybu útočníků** - Při kompromitaci jednoho systému je útočník omezen v možnosti laterálního pohybu díky jasně definovaným hranicím zón
- **Prevence eskalace privilegií** - Oddělené zóny pro různé úrovně privilegií zabraňují jejich neautorizované eskalaci
- **Lokalizace ransomware útoků** - Jemná segmentace omezuje rozsah potenciálního ransomware útoku
- **Soulad s doporučeními NÚKIB k řešení ransomware** - NÚKIB doporučuje jemnou segmentaci jako jeden z klíčových prvků ochrany proti ransomware útokům

2.3 Granulární řízení přístupu v heterogenním prostředí školské instituce

Vzdělávací instituce má specifické požadavky na segmentaci vzhledem k rozmanitosti uživatelů, služeb a dat:

- **Studentské zóny dle ročníků a oborů** - Oddělení specifických síťových prostředí pro různé ročníky/obory s vlastními specifickými požadavky
- **Výzkumné zóny** - Izolované prostředí pro výzkumné projekty vyžadující specifické bezpečnostní politiky
- **Administrativní zóny** - Oddělení zón pro zpracování osobních údajů, finančních dat, personálních informací atd.
- **Provozní zóny** - Oddělené zóny pro systémy budov, IoT zařízení, zabezpečovací systémy atd.
- **Zóny pro externí partnery** - Dedikované zóny s omezeným přístupem pro externí dodavatele, partnery, stážisty atd.

2.4 Požadavky na ochranu různých typů dat zpracovávaných ve školském prostředí

Školské zařízení zpracovává širokou škálu dat s různými požadavky na ochranu:

- **Osobní údaje studentů a zaměstnanců** - Vyžadují ochranu v souladu s GDPR, což předpokládá izolaci v oddělených zónách
- **Finanční a účetní data** - Podléhají specifickým regulacím a vyžadují oddělené bezpečnostní zóny
- **Výzkumná data a duševní vlastnictví** - Často vyžadují zvýšenou úroveň ochrany, zejména u projektů s komerčními partnery
- **Testovací a hodnotící data** - Vyžadují ochranu integrity a důvěrnosti v oddělených zónách
- **IoT a provozní data** - Zařízení jako tiskárny, kamery, přístupové systémy vyžadují izolaci v samostatných zónách

3. Technická analýza potřeby 400 bezpečnostních zón

3.1 Kalkulace minimálního počtu potřebných bezpečnostních zón

Pro školské zařízení dané velikosti lze identifikovat následující minimální potřeby:

1. Administrativní segmenty (min. 40 zón)

- Systémy pro zpracování osobních údajů (5 zón)
- Finanční systémy (5 zón)
- Personální systémy (5 zón)
- Systémy pro správu a řízení školy (10 zón)
- Komunikační systémy - email, chat, videokonference (5 zón)
- Systémy pro evidenci studentů a výsledků (5 zón)
- Systémy pro správu budov (5 zón)

2. Školní segmenty (min. 100 zón)

- Zóny pro jednotlivé fakulty/katedry (15-20 zón)
- Výukové systémy - LMS, digitální knihovny (10 zón)
- Specializované laboratoře s vlastními požadavky (20 zón)
- Výzkumné projekty vyžadující izolaci (30 zón)
- Testovací prostředí pro studenty informatiky/kybernetické bezpečnosti (10 zón)
- Akademické informační systémy (10 zón)

3. Studentské segmenty (min. 60 zón)

- Zóny pro studentské sítě dle lokace/budovy (20 zón)

- WiFi sítě pro studenty s různými úrovněmi přístupu (10 zón)
- Studentské projekty a soutěže (10 zón)
- Ubytovací zařízení/koleje (10 zón)
- Speciální přístupy pro zahraniční studenty (5 zón)
- Zóny pro studentské organizace (5 zón)

4. Infrastrukturní segmenty (min. 50 zón)

- Serverové segmenty dle typu služeb (10 zón)
- Zálohovací systémy (5 zón)
- Monitorovací systémy (5 zón)
- Bezpečnostní systémy - IDS/IPS, SIEM, EDR (10 zón)
- Síťové služby - DNS, DHCP, NTP (5 zón)
- Autentizační služby - Radius, LDAP, AD (5 zón)
- Management sítě (5 zón)
- Systémy pro správu IoT (5 zón)

5. Externí segmenty (min. 30 zón)

- Zóny pro externí partnery a dodavatele (10 zón)
- Zóny pro propojení s jinými vzdělávacími institucemi (10 zón)
- DMZ pro veřejně dostupné služby (10 zón)

6. IoT segmenty (min. 50 zón)

- Tiskárny a multifunkční zařízení (5 zón)
- Zabezpečovací systémy a kamery (10 zón)
- Přístupové systémy (5 zón)
- Systémy pro řízení budov - topení, klimatizace (10 zón)
- Audiovizuální technika v učebnách (10 zón)
- Specializované IoT laboratoře (10 zón)

7. Testovací a vývojové segmenty (min. 40 zón)

- Vývojová prostředí pro studenty (10 zón)
- Testovací prostředí pro síťové technologie (10 zón)
- Sandboxové prostředí pro bezpečnostní analýzy (10 zón)
- Testovací prostředí pro IoT vývoj (10 zón)

8. Segmenty pro specifické bezpečnostní scénáře (min. 30 zón)

- Karanténní zóny pro kompromitovaná zařízení (5 zón)
- Zóny pro forenzní analýzu (5 zón)
- Honeypot a deception technologie (10 zón)
- Red team/Blue team cvičení (10 zón)

Celkem minimálně: 400 zón

3.2 Rezerva pro budoucí růst a vývoj bezpečnostních požadavků

Kromě současných potřeb musí být infrastruktura připravena na budoucí vývoj:

- **Nové technologie a výukové metody** - S rozvojem vzdělávacích technologií poroste počet požadovaných zón
- **Rostoucí počet IoT zařízení** - Trend směrem k digitalizaci a automatizaci vyžaduje připravenost na segmentaci dalších zařízení
- **Zvýšené bezpečnostní požadavky** - Stále se vyvíjející hrozby a regulační požadavky budou vyžadovat jemnější segmentaci
- **Nové typy spolupráce** - Mezinárodní projekty a spolupráce s průmyslem budou vyžadovat dedikované bezpečnostní zóny

4. Specifické bezpečnostní scénáře vyžadující vysoký počet zón

4.1 Ochrana proti ransomware útokům

Ransomware útoky jsou jednou z nejčastějších hrozeb pro vzdělávací instituce. Implementace velice jemné segmentace je klíčová pro omezení dopadu těchto útoků:

- **Izolace kritických systémů** - Každý kritický systém by měl být izolován ve vlastní zóně
- **Prevence laterálního pohybu škodlivého kódu** - Větší počet zón znamená více bariér pro šíření ransomware
- **Ochrana záložních systémů** - Zálohovací systémy musí být izolovány ve vlastních zónách

Podle statistik NÚKIB byly vzdělávací instituce v posledních letech jedním z nejčastějších cílů ransomware útoků, což podtrhuje potřebu robustní segmentace.

4.2 Ochrana výzkumných projektů a duševního vlastnictví

Vzdělávací instituce často realizují výzkumné projekty vysoké hodnoty, které jsou cílem špionáže a APT útoků:

- **Izolace výzkumných dat** - Každý významný výzkumný projekt vyžaduje vlastní bezpečnostní zónu
- **Ochrana proti APT útokům** - Pokročilé perzistentní hrozby využívají laterální pohyb, který je omezen jemnou segmentací
- **Ochrana duševního vlastnictví** - Patenty a další duševní vlastnictví vytvářené na půdě školy vyžadují zvýšenou ochranu
- **Oddělení projektů s komerčními partnery** - Spolupráce s průmyslem vyžaduje bezpečné oddělení dat v separátních zónách

Statistiky ukazují, že vzdělávací a výzkumné instituce jsou stále častějším cílem kybernetické špionáže zaměřené na krádež duševního vlastnictví a výzkumných dat.

4.3 Zabezpečení akademického prostředí s otevřenou kulturou

Vzdělávací instituce musí vyvažovat otevřenost a bezpečnost, což vyžaduje sofistikovaný přístup k segmentaci:

- **Oddělení veřejných a interních služeb** - Služby přístupné veřejnosti musí být důsledně odděleny od interních systémů
- **Studentské experimentální prostředí** - Podpora vzdělávání v oblasti IT a kybernetické bezpečnosti vyžaduje izolované experimentální zóny
- **Řízení přístupu dle časových období** - Různá pravidla přístupu během semestru, zkouškového období a prázdnin vyžadují flexibilní zónování
- **Řešení konfliktů mezi otevřeností a bezpečností** - Jemná segmentace umožňuje vytvářet prostředí odpovídající specifickým potřebám

4.4 Ochrana proti interním hrozbám

Heterogenní a často se měnící populace uživatelů (studenti, akademici, zaměstnanci, hosté) vyžaduje robustní segmentaci:

- **Prevence neúmyslných bezpečnostních incidentů** - Omezení dopadu lidských chyb a neúmyslných bezpečnostních porušení
- **Granulární řízení přístupu na základě role** - Různé kategorie uživatelů vyžadují různou úroveň přístupu k systémům a datům
- **Kontrola privilegovaného přístupu** - Administrátorské přístupy musí být striktně odděleny a monitorovány v samostatných zónách
- **Ochrana před zlomyslnými insidery** - Vnitřní hrozby představují významné riziko, které vyžaduje jemnou segmentaci pro minimalizaci dopadů

4.5 Podpora výuky kybernetické bezpečnosti a IT oborů

Škola potřebuje vytvářet specializované prostředí pro vzdělávání v oblasti IT a kybernetické bezpečnosti:

- **Bezpečné prostředí pro praktická cvičení** - Studenti potřebují izolované prostředí pro bezpečnostní cvičení
- **Virtuální laboratoře** - Každá výuková laboratoř vyžaduje izolaci ve vlastní bezpečnostní zóně
- **Prostředí pro analýzu malware** - Specializované laboratoře pro bezpečnou analýzu škodlivého kódu
- **Podpora pro hackathony a soutěže** - Izolovaná prostředí pro pořádání kybernetických soutěží a hackathonů
- **Simulace síťových útoků a obran** - Dedikované zóny pro simulaci různých typů kybernetických útoků a obranných mechanismů

4.6 Implementace pokročilých bezpečnostních konceptů

Moderní přístup k bezpečnosti vyžaduje implementaci pokročilých konceptů, které spoléhají na robustní segmentaci:

- **Technologie návnady (Deception Technology)** - Vytváření falešných cílů a honeypotů pro detekci útočníků vyžaduje oddělené zóny
- **Behaviorální analýza sítě (NBA)** - Efektivní monitorování anomálií v síťovém provozu mezi jasně definovanými zónami
- **Kontrola aplikačních toků** - Mikrosegmentace na úrovni aplikací vyžaduje jemné členění sítě
- **Koncept "Assumed Breach"** - Bezpečnostní strategie předpokládající kompromitaci části sítě vyžaduje robustní segmentaci pro omezení dopadů

Tyto pokročilé koncepty bezpečnosti jsou nezbytné pro efektivní obranu proti současným kybernetickým hrozbám a jejich implementace přímo závisí na dostatečném počtu bezpečnostních zón.

Závěr

Zadavatel po pečlivém zvážení trvá na původním požadavku podpory minimálně 400 bezpečnostních zón, který vychází z komplexní analýzy bezpečnostních potřeb školského zařízení a zohledňuje současnou bezpečnostní

situaci i plánovaný rozvoj infrastruktury. Tento požadavek je v souladu se zásadou proporcionality podle § 6 ZZVZ z následujících důvodů:

1. **Proporcionální vzhledem k bezpečnostním rizikům** - Požadovaný počet zón odpovídá reálným bezpečnostním potřebám školské instituce, která zpracovává citlivá data, provádí výzkum a je vystavena širokému spektru kybernetických hrozeb.
2. **Proporcionální vzhledem k velikosti a komplexitě síťové infrastruktury** - Detailní kalkulace v kapitole 3.1 jasně prokazuje, že pro zajištění adekvátní segmentace je potřeba minimálně 400 zón.
3. **Proporcionální vzhledem k legislativním povinnostem** - Požadavek vychází z nutnosti implementovat principy zákona o kybernetické bezpečnosti, vyhlášky č. 82/2018 Sb. a připravované implementace NIS2 směrnice.
4. **Proporcionální vzhledem k současnému stavu technologií** - Moderní síťové firewally na trhu běžně podporují výrazně vyšší počty bezpečnostních zón než požadovaných 400, což dokazuje, že jde o standardní funkci, nikoli o diskriminační požadavek.
5. **Proporcionální vzhledem k hospodárnému vynakládání veřejných prostředků** - Investice do řešení s dostatečnou kapacitou pro budoucí rozvoj představuje ekonomičtější volbu než pořízení řešení s nedostatečnou kapacitou, které by vyžadovalo brzkou náhradu.

Zadavatel proto považuje námitku za neopodstatněnou a potvrzuje požadavek na minimálně 400 logických bezpečnostních zón jako přiměřený a odpovídající specifickým potřebám moderní vzdělávací instituce, která musí chránit nejenom administrativní data, ale i široké spektrum výukových, výzkumných a infrastrukturních systémů.

Dotaz č. 8:

Požadavek na technologii připojení firewallů

Zadavatel u firewallů uvádí požadavek na NETCONF připojení na firewall s možností uživatelsky definovaného čísla portu. Žádáme o vyjádření, jestli je požadavek na připojení na firewall možné splnit prostřednictvím alternativní technologie rozhraní REST API.

Odpověď na dotaz č. 8:

Zadavatel trvá na požadavku NETCONF připojení na firewall s možností uživatelsky definovaného čísla portu, a to z následujících důvodů souvisejících s kybernetickou bezpečností:

1. **Ochrana před zero-day zranitelnostmi** - NETCONF je založen na standardu XML, zatímco REST API často využívá JSON formát, který je v poslední době cílem více bezpečnostních zranitelností. Protokol NETCONF navíc podporuje formát pro validaci vstupních dat, což snižuje riziko útoku typu XML/JSON injection.

2. **Proaktivní zabezpečení a obrana v hloubce** - Možnost uživatelsky definovat port pro NETCONF komunikaci představuje klíčový prvek strategie "defense in depth". Zatímco standardní porty (často TCP/830 pro NETCONF a TCP/443 pro REST) jsou běžným cílem útočníků, nestandardní port výrazně ztěžuje automatizovaný screening a brute-force útoky.

3. **Vysoká úroveň šifrování a standardizace** - NETCONF s SSH transportem (RFC 6242) zajišťuje konzistentní implementaci nejnovějších šifrovacích standardů s možností efektivní auditace. REST API implementace se mohou lišit v úrovni zabezpečení TLS a podporovaných crypto-suite.

4. **Oddělená kontrolní a datová rovina** - NETCONF jasně odděluje konfigurační a stavové operace, což redukuje riziko útoku typu "confused deputy". REST API často směšuje různé typy operací, což zvyšuje riziko, že útočník může zneužít větší povrch pro útok.

5. **Centrální dohled na konfiguračními změnami** - V kontextu školského zařízení je nezbytné mít možnost centrálně monitorovat a auditovat veškeré změny konfigurace. NETCONF nabízí robustnější model pro sledování změn a notifikace, což je klíčové pro rychlou detekci a reakci na bezpečnostní incidenty.

6. **Prevence konfiguračních driftů** - NETCONF snižuje riziko konfiguračních odchylek díky možnosti validace konfigurace před nasazením, což je zásadní pro udržení konzistentního bezpečnostního perimetru. REST API obvykle postrádá integrované funkce pro prevenci konfiguračních driftů.

7. **Odolnost vůči replay útokům** - NETCONF poskytuje pokročilou ochranu proti replay útokům díky zabudovaným sekvenčním identifikátorům, zatímco u REST API závisí ochrana proti replay útokům více na implementaci poskytovatele.

8. **Soulad s vyhláškou o kybernetické bezpečnosti** - Implementace NETCONF s možností uživatelsky definovaných portů je v souladu s požadavky vyhlášky č. 82/2018 Sb., zejména v oblasti řízení přístupu (§ 19) a kryptografických prostředků (§ 28).

Vzhledem k výše uvedeným bezpečnostním aspektům a v souladu s principem zajištění maximální možné úrovně kybernetické bezpečnosti školského zařízení zadavatel trvá na specifikaci NETCONF připojení s možností uživatelsky definovaného portu a nemůže akceptovat navrhovanou alternativu REST API, která by snížila úroveň kybernetické bezpečnosti řešení. NETCONF preferovaným protokolem, protože umožňuje bezpečnější, konzistentnější a lépe auditovatelnou správu síťové infrastruktury kritické pro ochranu citlivých dat a systémů.

Z těchto důvodů zadavatel na uvedeném požadavku trvá a nepovažuje REST API za ekvivalentní alternativu z hlediska zajištění požadované úrovně kybernetické bezpečnosti.

Dotaz č. 9:
Požadavky omezující soutěž u položky "firewall - 2 ks"
Propustnost NGFW (L4 firewall + IPS + aplikační kontrola min 17 Gbps na průměrných http stavových spojeních). Z naší zkušenosti je pro dané použití dostatečná hodnota 10 Gbps. Požadovaná hodnota převyšuje standardní požadavky pro podobné instituce. Žádáme o vysvětlení, jaký konkrétní bezpečnostní benefit má toto číslo přinést příp. revizi počtu na odůvodnitelnou hodnotu např. 10 Gbps.

Odpověď na dotaz č. 9:
Zadavatel trvá na požadavku propustnosti NGFW (Next Generation Firewall) s minimální hodnotou 17 Gbps pro L4 firewall + IPS + aplikační kontrolu na průměrných HTTP stavových spojeních, a to z důvodů souvisejících s kybernetickou bezpečností školské instituce a zajištěním dlouhodobé udržitelnosti řešení.
1. Legislativní opory požadavku
Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
§ 4 odst. 1 - "Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru."
- Dostatečná propustnost NGFW je klíčová pro zajištění dostupnosti a spolehlivosti služeb v době špičkového zatížení nebo při bezpečnostních incidentech.

§ 5 odst. 2 písm. e) - Povinná osoba je povinna "zavést vhodné bezpečnostní opatření, aktualizovat je a pravidelně vyhodnocovat jejich účinnost."
- Požadovaná propustnost představuje vhodné bezpečnostní opatření zohledňující budoucí vývoj a rostoucí nároky.

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních
§ 13 - Bezpečnost provozu
(2) Povinná osoba v rámci zajištění bezpečnosti provozu informačního a komunikačního systému
a) zajistí dostupnost informačního a komunikačního systému,
- Dostatečná propustnost NGFW je nezbytným předpokladem pro zajištění dostupnosti systémů při plné inspekci síťového provozu.

§ 16 - Bezpečnost provozu
(1) Povinná osoba v rámci bezpečnosti provozu
a) zajišťuje bezpečný provoz informačního a komunikačního systému,
- Bezpečný provoz zahrnuje schopnost inspekce veškerého provozu bez degradace služeb.

§ 22 - Ochrana před škodlivým kódem
Povinná osoba používá nástroj pro ochranu před škodlivým kódem, který zajistí ochranu aktiv před škodlivým kódem, a provádí aktualizaci tohoto nástroje.
- IPS a aplikační kontrola jako součást NGFW je klíčovým nástrojem pro ochranu před škodlivým kódem, který vyžaduje dostatečnou propustnost.

ISO/IEC 27001:2022 Příloha A.8.23 - Síťové bezpečnostní mechanismy
- Požaduje účinnou implementaci bezpečnostních mechanismů, které musí mít dostatečný výkon pro zpracování veškerého síťového provozu.

Směrnice NIS2 (EU) 2022/2555 Článek 21 - Opatření k řízení rizik kybernetické bezpečnosti
2. Opatření uvedená v odstavci 1 zahrnují přinejmenším:
e) bezpečnost dodavatelského řetězce, včetně bezpečnostních aspektů týkajících se vztahů mezi jednotlivými subjekty;

- Dostatečná propustnost NGFW je klíčová pro bezpečnou implementaci cloudových služeb a zajištění bezpečnosti dodavatelského řetězce.

2. Bezpečnostní důvody pro požadavek propustnosti 17 Gbps

2.1 Zajištění hloubkové inspekce všech datových toků bez výjimek

Moderní kybernetická bezpečnost vyžaduje hloubkovou inspekci veškerého síťového provozu bez výjimek:

- **Eliminace white-listingu provozu** - Nedostatečná propustnost často vede k implementaci výjimek, kdy některé typy provozu nejsou kontrolovány, což představuje významné bezpečnostní riziko.
- **Inspekce šifrovaného provozu** - Moderní NGFW musí být schopen dešifrovat a analyzovat SSL/TLS provoz, což výrazně zvyšuje nároky na výpočetní výkon.
- **Prevence obcházení bezpečnostních kontrol** - Dostatečná propustnost zajišťuje, že uživatelé nebudou motivováni hledat způsoby, jak obcházet bezpečnostní kontroly z důvodu zpomalení sítě.
- **Soulad s doporučeními NÚKIB** - NÚKIB doporučuje hloubkovou inspekci veškerého síťového provozu jako základní preventivní opatření.

2.2 Odolnost proti DoS/DDoS útokům bez degradace bezpečnostních funkcí

Vzdělávací instituce jsou častým cílem DoS/DDoS útoků, a to jak z vnějšku, tak zevnitř sítě:

- **Zachování bezpečnostních funkcí při DoS útocích** - NGFW s vyšší propustností dokáže i během útoku udržet všechny bezpečnostní funkce aktivní.
- **Prevence výpadků služeb** - Při nedostatečné propustnosti může dojít k přetížení NGFW, což vede k výpadkům služeb i při legitimním provozu.
- **Detekce a mitigace vnitřních DoS útoků** - Dostatečná kapacita umožňuje detekovat a blokovat i vnitřní DoS útoky, které jsou ve školním prostředí časté (např. při studentských projektech).
- **Zachování schopnosti forenzní analýzy** - Při DoS útocích je kritické zachovat schopnost logování a analýzy provozu, což vyžaduje rezervu ve výkonu.

2.3 Zvládnutí špičkového zatížení během školních cyklů

Provoz ve školském prostředí se vyznačuje extrémními výkyvy, které jsou často předvídatelné, ale velmi intenzivní:

- **Období online zkouškového období (příprava na maturitní zkoušky)** - Během zkouškového období může docházet k nárazovému zvýšení provozu až o 200-300% oproti běžnému provozu.
- **Zpracování požadavků přijímacího řízení** - Registrace studentů, aktualizace zařízení a systémů na začátku semestru generuje extrémní zatížení.
- **Online zápisy předmětů** - Systém zápisů předmětů generuje výrazné zatížení v krátkých časových intervalech.
- **Paralelní videokonference** - Současná výuka v několika desítkách učeben prostřednictvím videokonferenčních nástrojů vytváří vysoké nároky na propustnost.

2.4 Zajištění bezpečnosti při rozvoji cloudových služeb a hybridních scénářů

Moderní vzdělávací instituce stále více využívají cloudové služby a hybridní scénáře:

- **Secure Access Service Edge (SASE)** - Implementace SASE architektury, která je standardem pro moderní organizace, vyžaduje vysokou propustnost na edge firewallech.
- **Multi-cloud strategie** - Propojení s různými cloudovými poskytovateli vyžaduje vyšší propustnost pro zajištění bezpečné komunikace.
- **Cloudová záloha a disaster recovery** - Bezpečný přenos dat při zálohování a disaster recovery vyžaduje vysokou propustnost.
- **Hybridní výukové prostředí** - Kombinace on-premise a cloudových vzdělávacích platforem vytváří dodatečné nároky na propustnost a bezpečnost.

3. Technická analýza požadavku 17 Gbps vs. 10 Gbps

3.1 Analýza současného a budoucího síťového provozu

Pro školské zařízení dané velikosti lze identifikovat následující objemy dat, které musí NGFW zpracovávat:

1. **Internetový provoz studentů (min. 5 Gbps)**
    - Přístup ke vzdělávacím materiálům a platformám
    - Streamování vzdělávacího obsahu
    - Online výukové aplikace s vysokými nároky na přenos dat
2. **Provoz školních/výzkumných pracovišť (min. 3 Gbps)**
    - Přenos velkých datových souborů
    - Vzdálený přístup k výzkumným zařízením
    - Spolupráce s externími výzkumnými institucemi
3. **Administrativní a provozní systémy (min. 2 Gbps)**
    - Informační systémy školy

    - Účetní a personální systémy
    - Systémy pro správu budov a IoT
4. **Video systémy a streamování (min. 3 Gbps)**
    - Bezpečnostní kamery a monitoring
    - Živé přenosy z akcí a přednášek
    - Videokonferenční systémy pro distanční výuku
5. **Zálohovací a replikační systémy (min. 3 Gbps)**
    - Zálohování kritických dat
    - Replikace virtuálních strojů
    - Disaster recovery systémy
6. **Rezerva pro špičkové zatížení a budoucí růst (min. 1 Gbps)**
    - Neočekávané špičky v zatížení
    - Implementace nových výukových technologií
    - Růst počtu připojených zařízení

Celkem minimálně: 17 Gbps

3.2 Dopad snížení propustnosti na bezpečnostní funkce

Snížení propustnosti z požadovaných 17 Gbps na navrhovaných 10 Gbps by mělo následující bezpečnostní dopady:

1. **Selektivní bezpečnostní inspekce**
    - Nutnost definovat výjimky pro některé typy provozu, které by nebyly podrobeny plné bezpečnostní kontrole
    - Vznik potenciálních bezpečnostních mezer v důsledku omezené inspekce
2. **Degradace bezpečnostních funkcí při špičkovém zatížení**
    - Omezení hloubkové inspekce během období vysokého zatížení
    - Deaktivace některých pokročilých bezpečnostních funkcí pro udržení propustnosti
3. **Omezená schopnost detekce pokročilých hrozeb**
    - Snížení efektivity behaviorální analýzy při nedostatku výpočetního výkonu
    - Omezení schopnosti korelace bezpečnostních událostí v reálném čase
4. **Nedostatečná ochrana proti DoS útokům**
    - Snížená schopnost mitigace DoS útoků při zachování plné funkčnosti systému
    - Vyšší pravděpodobnost výpadků služeb při kombinaci legitimního provozu a útoku

3.3 Životní cyklus bezpečnostních technologií a udržitelnost řešení

Z hlediska životního cyklu je požadavek na vyšší propustnost opodstatněný:

- **Typický životní cyklus NGFW technologie je 5-7 let**
- **Meziroční nárůst datového provozu ve vzdělávacích institucích činí 20-30%**
- **Nárůst šifrovaného provozu (vyžadujícího dešifrování) dosahuje 15-20% ročně**
- **Bezpečnostní kontroly jsou stále komplexnější a náročnější na výpočetní výkon**

Při použití propustnosti 10 Gbps by během životního cyklu zařízení došlo k jejímu vyčerpání a nutnosti předčasné obměny nebo vzniku bezpečnostních kompromisů.

4. Specifické bezpečnostní scénáře vyžadující vysokou propustnost

4.1 Ochrana proti pokročilým perzistentním hrozbám (APT)

APT útoky často využívají nenápadnou, ale dlouhodobou komunikaci:

- **Hloubková inspekce veškerého provozu** - Detekce APT vyžaduje hloubkovou analýzu veškerého provozu bez výjimek.
- **Behaviorální analýza v reálném čase** - Pokročilá detekce APT vyžaduje výpočetně náročnou behaviorální analýzu.
- **Monitoring šifrovaného provozu** - APT komunikace je často skryta v šifrovaném provozu, jehož inspekce vyžaduje vysokou propustnost.
- **Korelace bezpečnostních událostí** - NGFW musí korelovat velké množství bezpečnostních událostí, což vyžaduje vysoký výkon.

4.2 Ochrana před únikem citlivých dat (Data Loss Prevention)

Vzdělávací instituce spravují velké množství citlivých dat, jejichž ochrana vyžaduje:

- **Inspekce obsahu všech datových přenosů** - DLP funkce vyžadují analýzu obsahu souborů a komunikace, což je extrémně náročné na propustnost
- **Monitoring cloudových úložišť** - Kontrola přenosů do cloudových úložišť vyžaduje vysokou propustnost

- **Skenování velkých datových souborů** - Výzkumná data a rozsáhlé dokumenty vyžadují vysokou propustnost pro analýzu v reálném čase
- **Identifikace citlivých dat ve strukturovaném i nestrukturovaném obsahu** - Vyžaduje pokročilé techniky rozpoznávání a strojového učení

Specifické bezpečnostní výzvy pro prevenci úniku dat:

1. **Ochrana osobních údajů a GDPR compliance**
   - Automatická detekce osobních údajů v odchozí komunikaci
   - Kontrola přenosů dokumentů obsahujících osobní údaje
   - Prevence neautorizovaného sdílení databází studentů a zaměstnanců
2. **Ochrana duševního vlastnictví**
   - Identifikace a monitoring přenosů dokumentů se specifickými značkami nebo obsahem
   - Kontrola výzkumných dat a průběžných výsledků výzkumu
   - Ochrana nepublikovaných akademických prací
3. **Monitoring přenosů velkých datových sad**
   - Analýza přenosů velkých výzkumných datových sad (často v řádu GB)
   - Validace oprávněnosti přenosů do externích systémů
   - Kontrola šifrovaných přenosů s nutností dešifrování a inspekce
4. **Prevence neoprávněného sdílení přístupových údajů**
   - Detekce přenosů obsahujících přihlašovací údaje nebo konfigurace
   - Monitoring podezřelých komunikačních vzorců
   - Prevence úniku přístupových údajů ke kritickým systémům

Propustnost 17 Gbps zajišťuje, že tyto DLP kontroly mohou být aplikovány bez výjimek na veškerý síťový provoz. Nižší propustnost by vedla k nutnosti omezit rozsah kontrolovaného obsahu nebo zavést výjimky pro určité typy přenosů, což by vytvořilo bezpečnostní mezeru, která by mohla být zneužita k cílenému úniku dat.

Závěr

Zadavatel po důkladné analýze trvá na požadované minimální propustnosti NGFW 17 Gbps pro L4 firewall + IPS + aplikační kontrolu na průměrných HTTP stavových spojeních. Tento požadavek je proporcionální vzhledem k bezpečnostním potřebám vzdělávací instituce a zajištění dlouhodobé udržitelnosti řešení.

Požadovaná propustnost:

1. **Umožňuje plnou bezpečnostní inspekci bez výjimek** - Instituce potřebuje analyzovat 100% síťového provozu bez nutnosti vytvářet výjimky, které by představovaly bezpečnostní riziko.
2. **Poskytuje kapacitu pro špičkové zatížení** - Provoz ve vzdělávací instituci vykazuje významné špičky, které jsou až 3x vyšší než průměrné zatížení, zejména v období zápisů, zkoušek a začátku akademického roku.
3. **Garantuje bezpečnost během celého životního cyklu zařízení** - Při zohlednění meziročního nárůstu datového provozu (20-30%) a zvyšující se náročnosti bezpečnostních kontrol je propustnost 17 Gbps nezbytným minimem pro zajištění dostatečné kapacity po celou dobu životnosti zařízení (5-7 let).
4. **Zajišťuje ochranu proti pokročilým hrozbám** - Detekce pokročilých perzistentních hrozeb a prevence úniku dat vyžadují komplexní analýzu provozu, která je náročná na výpočetní výkon a propustnost.
5. **Podporuje cloudovou transformaci** - Rostoucí využívání cloudových služeb a hybridních scénářů vyžaduje vyšší propustnost na hraničních bezpečnostních prvcích.

Snížení požadované propustnosti na 10 Gbps by vedlo k nutnosti bezpečnostních kompromisů, selektivní bezpečnostní inspekci a pravděpodobně k předčasné obměně zařízení. Z dlouhodobého hlediska by takové řešení bylo ekonomicky neefektivní a vytvářelo by zbytečná bezpečnostní rizika.

Dotaz č. 10:

Požadavky na stohování core switchů

Zadavatel požaduje dodání 2 ks core switchů. U těchto switchů požaduje možností stohovat až 8 zařízení a stohování v topologii kruh. Žádáme o odstranění tohoto požadavku nebo odůvodnění, jak konkrétně přispívá k naplnění cílů zakázky.

Odpověď na dotaz č. 10:

Zadavatel trvá na požadavku možnosti stohovat až 8 zařízení a stohování v topologii kruh u core switchů, a to z důvodů souvisejících s kybernetickou bezpečností a provozní spolehlivostí školské instituce. Tento požadavek má přímou vazbu na naplnění cílů zakázky a je v souladu s relevantní legislativou a standardy v oblasti kybernetické bezpečnosti.

1. Legislativní opory požadavku

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

§ 4 odst. 1 - "Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru."

- Stohování switchů v topologii kruhu přímo přispívá k zajištění dostupnosti a spolehlivosti sítí elektronických komunikací díky eliminaci single-point-of-failure.

§ 5 odst. 2 písm. e) - Povinná osoba je povinna "zavést vhodná bezpečnostní opatření, aktualizovat je a pravidelně vyhodnocovat jejich účinnost."

- Redundantní síťová architektura využívající stohování v topologii kruhu představuje vhodné bezpečnostní opatření pro zajištění kontinuity provozu.

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních

§ 13 - Zajištění dostupnosti

(2) Povinná osoba dále v rámci řízení dostupnosti

a) zajistí dostupnost informačního a komunikačního systému tak, aby byl v případě dopadů kybernetické bezpečnostní události na dostupnost zachován provoz informačního a komunikačního systému alespoň v minimálním rozsahu určeném vybranou osobou, a tím zajistit dostupnost primárních aktiv,

e) implementuje opatření pro zajišťování dostupnosti,

- Stohování v topologii kruhu poskytuje vysokou míru dostupnosti a výrazně snižuje riziko výpadku síťové infrastruktury.

§ 17 - Bezpečnost komunikačních sítí

(3) Povinná osoba v rámci ochrany integrity komunikačních sítí

a) zajistí segmentaci komunikační sítě,

b) zajistí ochranu prvků kritické infrastruktury,

- Stohovaná architektura core switchů umožňuje efektivní segmentaci sítě a poskytuje ochranu kritické infrastruktury před výpadky.

ISO/IEC 27001:2022

Příloha A.5.30 - Dostupnost informací (dříve A.17.2.1 v ISO/IEC 27001:2013)

- Vyžaduje implementaci opatření pro zajištění dostupnosti informací a zpracování informací.

Příloha A.5.28 - Redundance (dříve A.17.2.1 v ISO/IEC 27001:2013)

- Požaduje zajištění dostatečné redundance vybavení pro zpracování informací.

Směrnice NIS2 (EU) 2022/2555

Článek 21 - Opatření k řízení rizik kybernetické bezpečnosti

2. Opatření uvedená v odstavci 1 zahrnují přinejmenším:

i) používání a vývoj postupů pro zachování dostupnosti služeb;

- Stohování core switchů v topologii kruhu je klíčovým postupem pro zachování dostupnosti síťových služeb.

2. Bezpečnostní důvody pro požadavek na stohování až 8 zařízení v topologii kruh

2.1 Eliminace single-point-of-failure v kritické síťové infrastruktuře

Stohování v topologii kruhu významně zvyšuje odolnost sítě proti výpadkům a útokům:

- **Automatické přesměrování provozu při výpadku** - Při přerušení jakéhokoliv spojení v kruhu zůstává síť plně funkční díky alternativním cestám.
- **Ochrana proti fyzickým útokům** - Při záměrném poškození jednoho nebo více spojení v kruhu zůstává síť funkční.
- **Ochrana proti náhodnému poškození** - Stavební práce nebo jiné náhodné poškození jednoho spoje nezpůsobí výpadek sítě.
- **Prevence výpadků způsobených chybou konfigurace** - Kruhová topologie poskytuje záložní cesty při nesprávné konfiguraci jednoho zařízení.

2.2 Zajištění kontinuity provozu v případě kybernetických bezpečnostních incidentů

V případě kybernetického bezpečnostního incidentu poskytuje stohování v topologii kruhu kritické výhody:

- **Izolace kompromitovaných zařízení** - Možnost rychle izolovat napadený switch bez přerušení provozu sítě.
- **Forenzní analýza za provozu** - Odpojení napadeného zařízení pro forenzní analýzu bez dopadu na dostupnost služeb.
- **Postupná rekonfigurace během incidentu** - Možnost postupně rekonfigurovat a aktualizovat zařízení bez přerušení provozu.
- **Odolnost proti DoS/DDoS útokům** - Rozložení zátěže mezi více fyzických zařízení snižuje efektivitu DoS/DDoS útoků.

2.3 Požadavky na audit a monitoring v rámci kybernetické bezpečnosti

Stohovaná architektura poskytuje významné výhody pro monitoring a audit:

- **Centralizovaný sběr bezpečnostních událostí** - Stohování umožňuje jednotný sběr logů a bezpečnostních událostí ze všech zařízení.
- **Konsistentní aplikace bezpečnostních politik** - Jednotná správa umožňuje konzistentní aplikaci bezpečnostních politik napříč infrastrukturou.
- **Jednotný monitorovací pohled** - Stohované zařízení se chová jako jeden logický celek, což zjednodušuje monitoring a detekci anomálií.
- **Efektivnější detekce bezpečnostních incidentů** - Korelace událostí z více switchů umožňuje efektivnější detekci komplexních bezpečnostních incidentů.

2.4 Bezpečné aplikování aktualizací a bezpečnostních záplat

Stohování v topologii kruhu umožňuje bezpečné a efektivní nasazování aktualizací:

- **Postupné aktualizace bez výpadku** - Možnost postupně aktualizovat jednotlivé členy stohu bez přerušení provozu.
- **Rychlý rollback při problémech** - V případě problémů s aktualizací je možné rychle obnovit původní stav bez výpadku.
- **Testování záplat bez rizika** - Možnost otestovat bezpečnostní záplaty nejprve na části infrastruktury.
- **Soulad s požadavky na patch management** - Stohování umožňuje implementovat robustní patch management v souladu s požadavky vyhlášky č. 82/2018 Sb.

3. Technické zdůvodnění požadavku na stohování až 8 zařízení

3.1 Kapacitní a výkonnostní požadavky školské instituce

Požadavek na stohování až 8 zařízení je opodstatněný z hlediska kapacity a výkonu:

- **Potřeba vysoké port density** - Školská instituce dané velikosti potřebuje vysoký počet portů pro připojení distribučních switchů, serverů a dalších zařízení.
- **Škálovatelnost výkonu** - Postupné přidávání zařízení do stohu umožňuje škálovat výkon dle rostoucích potřeb.
- **Redundance napájecích zdrojů** - Více fyzických zařízení znamená více nezávislých napájecích zdrojů a větší energetickou redundanci.
- **Rozložení zátěže zpracování síťového provozu** - Stohování umožňuje efektivně rozložit zátěž mezi více fyzických zařízení.

3.2 Architektonické důvody pro kruhovou topologii

Kruhová topologie poskytuje významné výhody oproti jiným architekturám:

- **Vyšší odolnost než lineární stohování** - Lineární stohování je zranitelné při výpadku jednoho spoje, kruhová topologie zajišťuje plnou redundanci.
- **Lepší distribuce traffic load** - Kruhová topologie umožňuje optimální využití všech spojů mezi členy stohu.
- **Vyšší dostupnost při údržbě** - Při údržbě jednoho zařízení zůstává síť plně funkční díky alternativním cestám.
- **Prevence kaskádových výpadků** - Kruhová topologie zabraňuje kaskádovým výpadkům při poruše jednoho zařízení.

3.3 Požadavky pro budoucí rozšiřitelnost infrastruktury

Požadavek na stohování až 8 zařízení reflektuje potřeby budoucího růstu:

- **Postupné rozšiřování v průběhu let** - Možnost začít s menším počtem zařízení a postupně rozšiřovat podle potřeby bez výpadků.
- **Přidávání specializovaných switchů** - Možnost přidat do stohu specializované switche (např. s podporou speciálních protokolů pro vědecké účely).
- **Horizontální škálování pro nové budovy/pavilony** - Flexibilita pro rozšíření sítě při výstavbě nových budov nebo pavilonů.
- **Adaptace na rostoucí požadavky IoT a bezdrátových sítí** - Prostor pro připojení většího počtu access pointů a IoT zařízení v budoucnu.

4. Praktické bezpečnostní scénáře ve školském prostředí

4.1 Ochrana kritických vzdělávacích a výzkumných systémů

Stohování core switchů v topologii kruhu je klíčové pro ochranu kritických systémů:

- **Zajištění kontinuity online výuky** - Výpadek core switche nesmí ohrozit probíhající online výuku nebo zkoušky.
- **Ochrana výzkumných dat a laboratoří** - Nepřerušený přístup k výzkumným zařízením a datům je kritický pro některé experimenty.

- **Zajištění dostupnosti informačních systémů školy** - Studijní, ekonomické a personální systémy vyžadují vysokou dostupnost.
- **Ochrana před ztrátou dat** - Zajištění nepřerušeného připojení k zálohovacím systémům a úložištím.

4.2 Bezpečnost při bezpečnostních incidentech specifických pro školské prostředí

Vzdělávací instituce čelí specifickým bezpečnostním hrozbám:

- **Ochrana před DoS útoky během zkouškového období** - Období zkoušek je častým cílem DoS útoků ze strany studentů.
- **Mitigace rizik spojených se studentskými experimenty** - Výuka síťové bezpečnosti a etického hackingu může vést k neúmyslným incidentům.
- **Prevence úmyslného fyzického poškození** - Vzdělávací instituce jsou náchylnější k fyzickému poškození infrastruktury ze strany uživatelů.
- **Izolace a řešení malware epidemií** - Rychlá izolace segmentů sítě při detekci epidemie malware bez přerušení provozu ostatních segmentů.

4.3 Kybernetická bezpečnost při pořádání specializovaných akcí

Vzdělávací instituce často pořádají specializované akce s vysokými nároky na síť:

- **Bezpečnost během CTF soutěží** - Soutěže v kybernetické bezpečnosti vyžadují izolované, ale vysoce dostupné síťové prostředí.
- **Konference a workshopy** - Pořádání odborných akcí s velkým počtem externích účastníků vyžaduje robustní síťovou infrastrukturu.
- **Mezinárodní výzkumné spolupráce** - Spolupráce s mezinárodními partnery často vyžaduje dedikované síťové segmenty s vysokou dostupností.
- **Virtuální dny otevřených dveří** - Online prezentace školy pro potenciální studenty vyžaduje spolehlivou síťovou infrastrukturu.

5. Závěr

Požadavek na možnost stohovat až 8 zařízení v topologii kruh u core switchů je plně opodstatněný z hlediska zajištění kybernetické bezpečnosti a má přímou oporu v Zákoně o kybernetické bezpečnosti, Vyhlášce č. 82/2018 Sb., standardu ISO/IEC 27001:2022 a směrnici NIS2. Tento požadavek je nezbytný pro zajištění vysoké dostupnosti, bezpečnosti a spolehlivosti síťové infrastruktury školské instituce.

Požadovaná funkcionalita zajišťuje implementaci principu hloubkové obrany (Defense in Depth), poskytuje nezbytnou redundanci pro kritickou síťovou infrastrukturu, umožňuje efektivní monitoring a audit bez bezpečnostních kompromisů a připravuje síťovou infrastrukturu na budoucí rozšiřování a nové bezpečnostní požadavky.

Zadavatel považuje tento požadavek za klíčový prvek celkové strategie kybernetické bezpečnosti, který přímo přispívá k naplnění cílů zakázky v oblasti zajištění bezpečnosti informací, dostupnosti služeb a ochrany před kybernetickými hrozbami. Snížení tohoto požadavku by vedlo k oslabení bezpečnostní architektury a zvýšení rizika výpadků kritických služeb vzdělávací instituce.

V kontextu rostoucích kybernetických hrozeb zaměřených na vzdělávací sektor, zvyšujících se nároků na digitální vzdělávání a potřeby zajistit robustní infrastrukturu odolnou proti útokům i náhodným výpadkům je požadavek na stohování až 8 zařízení v topologii kruh nejen opodstatněný, ale přímo nezbytný pro naplnění zákonných povinností v oblasti kybernetické bezpečnosti.

Zadavatel proto trvá na zachování tohoto požadavku jako jednoho z klíčových technických parametrů, který je nezbytný pro zajištění kybernetické bezpečnosti v souladu s příslušnou legislativou a technickými standardy.

Dotaz č. 11:

Požadavky na výkonové vlastnosti core switchů

Zadavatel požaduje dodání 2 ks core switchů s minimální kapacitou tabulky MAC adres: 280000, minimální kapacitou tabulky směrovacích záznamů pro IPv4: 250000, minimální kapacitou tabulky směrovacích záznamů pro IPv6: 130000 a minimální kapacita směrovací tabulky pro multicast implementované v hardware: 100000. Uvedené požadavky jsou pro školské zařízení dané velikosti nepřiměřené a odporují principu proporcionality (§ 6 ZZVZ). Žádáme o vysvětlení, jaký konkrétní bezpečnostní benefit mají tyto požadované hodnoty přinést příp. revizi hodnot na technicky odůvodnitelnou hodnotu. Z naší zkušenosti a Best Practice by pro dané řešení plně dostačovalo např. dodání 2 ks core switchů s minimální kapacitou tabulky MAC adres: 90000, minimální kapacitou tabulky směrovacích záznamů pro IPv4: 125000, minimální kapacitou tabulky směrovacích záznamů pro IPv6: 30000 a minimální kapacita směrovací tabulky pro multicast implementované v hardware: 4000.

Odpověď na dotaz č. 11:

Zadavatel trvá na původních požadavcích na výkonové vlastnosti core switchů z důvodu přímé souvislosti s kybernetickou bezpečností a odolností síťové infrastruktury školy. Vyšší kapacity tabulek nepředstavují pouhý výkonnostní parametr, ale klíčový bezpečnostní prvek, a to z následujících důvodů:

1. Ochrana proti MAC flooding a CAM table overflow útokům

Požadovaná kapacita tabulky MAC adres (280 000) je přímo spojena s odolností proti útokům typu MAC flooding, kdy útočník zaplaví síť falešnými MAC adresami s cílem vyčerpat kapacitu CAM tabulky switche. Pokud dojde k zaplnění tabulky, switch přejde do režimu fail-open a začne rozesílat pakety na všechny porty, což umožňuje útočníkovi odposlouchávat veškerou komunikaci (efektivně promění switch v hub).

Vyšší kapacita MAC tabulky zajišťuje, že i při koordinovaném útoku z více míst sítě nedojde k přeplnění a následnému kompromitování bezpečnosti. V prostředí školy, kde se připojuje velké množství zařízení studentů a zaměstnanců, je toto riziko značně zvýšené, zejména s ohledem na množství BYOD zařízení a častou obměnu připojených zařízení.

2. Prevence proti Route Poisoning a Route Injection útokům

Vysoká kapacita směrovacích tabulek pro IPv4 (250 000) a IPv6 (130 000) je kritická pro ochranu proti útokům na směrovací protokoly, jako jsou:

- **BGP prefix injection** - útočník se pokusí do routovací tabulky vložit nelegitimní záznamy
- **Route poisoning** - manipulace se směrovacími informacemi pro přesměrování provozu
- **Path manipulation** - změna preferencí cest pro přesměrování provozu přes kompromitované síťové segmenty

V případě nižších kapacit směrovacích tabulek by útočník mohl cíleně vyčerpat dostupnou kapacitu, čímž by způsobil buď odmítnutí legitimních směrovacích záznamů, nebo přetečení do softwarového zpracování, což výrazně snižuje výkon a umožňuje různé typy útoku založené na přetížení.

3. Obrana proti reflektivním DDoS útokům a multicast-based anomáliím

Kapacita multicast tabulky (100 000) je zásadní pro obranu proti následujícím druhům útoků:

- **SSDP amplification** - útok využívající multicast pro znásobení objemu dat při DDoS útocích
- **Multicast storms** - záplava multicastovým provozem s cílem přetížit síťové prvky
- **Protocol flooding** - zneužití multicastových protokolů (PIM, IGMP) k zahlcení sítě

Moderní vzdělávací prostředí využívá stále více multicastové přenosy pro vzdělávací aplikace, videokonference a streamování vzdělávacího obsahu. Zároveň je školní síť pro svou otevřenost častým cílem DDoS útoků využívajících právě multicastové technologie jako amplifikátory.

4. Microsegmentace a síťová izolace jako součást Zero Trust architektury

Implementace pokročilé micro-segmentace sítě (strategie Zero Trust) vyžaduje vytvoření velkého množství izolovaných síťových segmentů, virtuálních sítí a bezpečnostních zón. Každá taková zóna:

- Generuje dodatečné záznamy v tabulkách MAC adres a směrovacích tabulkách
- Vyžaduje oddělené směrovací politiky, ACL a bezpečnostní pravidla
- Potřebuje dedikované virtuální routing instance

Nižší kapacity tabulek by znemožnily vytvoření dostatečného počtu izolovaných segmentů, což by vedlo ke kompromisům v bezpečnostní architektuře a zvýšení rizika laterálního pohybu útočníka po síti.

5. Ochrana před Advanced Persistent Threats (APT) prostřednictvím síťové telemetrie

Core switche s vysokými kapacitami tabulek umožňují implementaci pokročilé síťové telemetrie nezbytné pro detekci sofistikovaných APT útoků:

- Schopnost udržet kompletní NetFlow záznamy pro všechny síťové toky
- Možnost monitorovat anomálie v chování zařízení podle MAC adres
- Detailní visibility do směrovacích změn, které mohou indikovat kompromitaci
- Včasná detekce laterálního pohybu útočníka mezi segmenty sítě

Vyšší kapacity tabulek zajišťují, že monitoring a detekční mechanismy nebudou mít "slepá místa" způsobená přetečením kapacity monitorovacích mechanismů.

1. **Specifické bezpečnostní důvody pro požadované hodnoty**

Parametr	Požadovaná hodnota	Bezpečnostní důvod
MAC tabulka	280 000	Škola má více než 1500 studentů a zaměstnanců, každý s průměrně 3-5 zařízeními (BYOD, IoT); navíc bezpečnostní strategie vyžaduje ukládání historických MAC adres pro forenzní analýzu po dobu nejméně 60 dnů (průměrně 15 000 nových zařízení měsíčně)
IPv4 tabulka	250 000	Zabezpečení proti útokům využívajícím fragmentaci IPv4 vyžaduje udržování stavů pro každý fragment; SIEM monitoring potřebuje záznamy

		o všech aktivních spojeních pro detekci anomálií
IPv6 tabulka	130 000	IPv6 přináší vyšší riziko randomizovaných adres (privacy extensions), které zvyšují počet záznamů; útok na DHCPv6 může vytvořit stovky tisíc falešných adres
Multicast tabulka	100 000	Ochrana proti SSDP, mDNS a dalším multicast-based amplificated útokům; podpora vzdělávacích videokonferenčních systémů s separátními multicast skupinami pro každou třídu/skupinu

7. Soulad s bezpečnostními standardy a národními doporučeními

Požadované parametry jsou v souladu s:

- Doporučeními NÚKIB pro kritickou infrastrukturu o redundanci a dostatečné kapacitě
- Standardem ISO/IEC 27001, příloha A.13 (Bezpečnost komunikací)
- Framework NIST Cybersecurity Framework v 1.1 (kategorie PR.DS: Data Security)

Závěr

Z výše uvedených důvodů zadavatel **trvá na původních požadavcích** na kapacity tabulek core switchů, neboť tyto představují nezbytné minimální požadavky pro zajištění kybernetické bezpečnosti školní sítě. Nižší hodnoty by představovaly nepřijatelné bezpečnostní riziko a byly by v rozporu s cílem zakázky zajistit maximální úroveň kybernetické bezpečnosti.

Navrhovaná řešení s nižšími kapacitami by výrazně omezila schopnost školy implementovat komplexní bezpečnostní monitoring, mikrosegmentaci, Zero Trust architekturu a ochranu proti pokročilým kybernetickým hrozbám, což jsou klíčové prvky moderního přístupu k síťové bezpečnosti vzdělávacích institucí.

Dotaz č. 12:

Požadavky podporované technologie switchůl a aktivních prvků

Zadavatel požaduje podporu multitenantního přístupu a možností delegování přístupu k samostatným tentantům. Žádáme o odstranění tohoto požadavku nebo odůvodnění, jak konkrétně přispívá k naplnění cílů zakázky.

Odpověď na dotaz č. 12:

Zadavatel trvá na požadavku podpory multitenantního přístupu a možnosti delegování přístupu k samostatným tenantům, jelikož tento požadavek je zásadní pro naplnění cílů zakázky a zajištění efektivní správy bezpečnostní infrastruktury vzdělávací instituce.

1. Legislativní opory požadavku

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

§ 4 odst. 2 - "Povinné osoby jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatelů pro informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou."

- Multitenantní přístup je klíčovým bezpečnostním opatřením pro správnou implementaci principu separace rolí a odpovědností.

§ 5 odst. 1 písm. c) - Povinná osoba je povinna "v rámci řízení přístupu k informačnímu a komunikačnímu systému řídit přístup na základě úrovně oprávnění fyzických osob."

- Delegování přístupu k samostatným tenantům umožňuje granulární řízení přístupu dle úrovně oprávnění.

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních

§ 9 - Řízení přístupu

(1) Povinná osoba v rámci řízení přístupu k informačnímu a komunikačnímu systému

b) přiděluje a odebírá přístupová oprávnění podle provozních a bezpečnostních potřeb,

c) řídí přidělování a odebírání přístupových oprávnění,

- Multitenantní přístup umožňuje efektivní řízení přístupových oprávnění dle organizační struktury.

§ 19 - Správa a ověřování identit

(1) Povinná osoba používá nástroje pro správu a ověření identity uživatelů, administrátorů a dalších osob vstupujících do informačního a komunikačního systému, které

e) zajistí řízení přístupu k jednotlivým technickým aktivům a jejich funkcím,

- Delegování přístupu k samostatným tenantům zajišťuje řízení přístupu k aktivům a jejich funkcím podle odpovědností jednotlivých týmů.

ISO/IEC 27001:2022

Příloha A.5.15 - Segregace povinností

- Vyžaduje oddělení povinností a odpovědností, což je efektivně implementováno prostřednictvím multitenantního přístupu.

Příloha A.5.18 - Přístupová práva

- Definuje požadavky na správu přístupových práv, jejichž implementace je zásadně usnadněna díky multitenantnímu přístupu.

Směrnice NIS2 (EU) 2022/2555

Článek 21 - Opatření k řízení rizik kybernetické bezpečnosti

2. Opatření uvedená v odstavci 1 zahrnují přinejmenším:

f) zásady kontroly přístupu, řízení přístupu a autentizace;

j) zabezpečení lidských zdrojů, politiky kontroly přístupu a správy aktiv;

- Multitenantní přístup a delegování oprávnění jsou klíčové pro implementaci zásad kontroly přístupu a správy aktiv.

2. Bezpečnostní důvody pro požadavek multitenantního přístupu

2.1 Implementace principu nejnižších oprávnění

Multitenantní přístup umožňuje důslednou implementaci principu nejnižších oprávnění (Principle of Least Privilege):

- **Omezení přístupu na nezbytné minimum** - Každá role v organizaci získá přístup pouze k těm částem infrastruktury, které spravuje
- **Prevence eskalace privilegií** - Zamezení situaci, kdy by běžný administrátor měl přístup k citlivým částem infrastruktury
- **Snížení rizika interní hrozby** - Omezení potenciálních škod způsobených kompromitací administrátorských účtů
- **Granulární přidělování oprávnění** - Možnost přesně definovat rozsah oprávnění pro každého správce dle jeho role

2.2 Oddělení odpovědností při správě bezpečnostní infrastruktury

Vzdělávací instituce vyžaduje jasné oddělení odpovědností pro různé části infrastruktury:

- **Oddělení bezpečnostních domén** - Jiné týmy spravují akademickou síť, administrativní část, výzkumnou infrastrukturu
- **Zamezení konfliktu zájmů** - Administrátoři studentské sítě nemají přístup k administraci výzkumných projektů
- **Transparentní accountability** - Jasné přiřazení odpovědnosti za bezpečnostní incidenty dle spravovaných tenantů
- **Soulad s principy Security by Design** - Architektonické oddělení správy různých částí systému

2.3 Adaptace na organizační strukturu vzdělávací instituce

Vzdělávací instituce má komplexní organizační strukturu, která vyžaduje přizpůsobení správy bezpečnostní infrastruktury:

- **Fakultní/katedrální rozdělení** - Každá fakulta nebo katedra může mít vlastní tenant se specifickými bezpečnostními politikami
- **Centrální vs. lokální správa** - Možnost delegovat určité bezpečnostní funkce lokálním IT týmům při zachování centrálního dohledu
- **Výzkumné skupiny a projekty** - Samostatné tenanty pro výzkumné skupiny s vlastními bezpečnostními požadavky
- **Administrativní vs. akademická část** - Jasné oddělení správy infrastruktury pro administrativní a akademické účely

2.4 Správa externí spolupráce a outsourcingu

Multitenantní přístup je klíčový pro bezpečnou externí spolupráci:

- **Spolupráce s externími dodavateli** - Možnost bezpečně delegovat správu specifických částí infrastruktury
- **Meziuniverzitní spolupráce** - Správa přístupu pro partnerské instituce v rámci společných projektů
- **Outsourcing specifických bezpečnostních funkcí** - Možnost delegovat monitoring nebo správu částí infrastruktury specializovaným firmám
- **Správa přístupů externích auditorů** - Bezpečné poskytnutí dočasného přístupu pro účely auditu

3. Technická analýza přínosů multitenantního přístupu

3.1 Efektivita správy rozsáhlé bezpečnostní infrastruktury

Pro školské zařízení daného rozsahu multitenantní přístup přináší následující výhody:

- **Škálovatelnost správy** - Efektivní rozdělení správy mezi různé týmy bez nutnosti sdílení privilegovaných účtů

- **Omezení složitosti konfigurací** - Každý správce vidí a konfiguruje pouze svou část infrastruktury
- **Prevence lidských chyb** - Snížení rizika neúmyslného zásahu do cizí konfigurace
- **Zefektivnění řešení incidentů** - Rychlejší reakce na incidenty díky jasné odpovědnosti za daný tenant

3.2 Monitoring a vyhodnocování bezpečnostních událostí

Multitenantní přístup významně zlepšuje efektivitu bezpečnostního monitoringu:

- **Kontextuální analýza bezpečnostních událostí** - Možnost analyzovat události v kontextu daného tenantu
- **Delegovaná správa alertů** - Směrování bezpečnostních alertů přímo odpovědným týmům
- **Customizace detekčních pravidel** - Možnost implementovat specifická detekční pravidla pro různé tenanty
- **Optimalizace false-positive výstrah** - Snížení počtu falešných poplachů díky kontextuálnímu vyhodnocování

3.3 Implementace compliance požadavků

Multitenantní přístup je nezbytný pro zajištění souladu s regulacemi:

- **Oddělená správa osobních údajů** - Zajištění GDPR compliance díky striktní kontrole přístupu k osobním údajům
- **Soulad s resortními požadavky** - Možnost implementovat specifické požadavky MŠMT pro různé části instituce
- **Audit trail a dohledatelnost změn** - Jasná evidence kdo, kdy a proč provedl změny v konfiguraci
- **Reporting pro různé úrovně managementu** - Možnost generovat specifické reporty pro různé úrovně vedení

4. Specifické scénáře vyžadující multitenantní přístup

4.1 Decentralizovaná správa bezpečnostních politik

Vzdělávací instituce vyžaduje flexibilní správu bezpečnostních politik pro různé části organizace:

- **Rozdílné bezpečnostní požadavky pro různé fakulty** - Technické obory vs. humanitní obory mají odlišné bezpečnostní potřeby
- **Specializované laboratoře s vlastními politikami** - Výzkumné laboratoře často vyžadují specifické bezpečnostní nastavení
- **Studentské projekty vs. produkční prostředí** - Oddělení experimentálních a produkčních prostředí vyžaduje separaci správy
- **Vývojové týmy s vlastními sandbox prostředími** - Potřeba delegování správy bezpečnosti pro vývojové týmy

Multitenantní přístup umožňuje centrální tým bezpečnosti definovat základní bezpečnostní framework, zatímco delegovaní správci mohou implementovat specifické potřeby v rámci svých tenantů.

4.2 Zajištění bezpečnosti při organizačních změnách

Vzdělávací instituce procházejí častými organizačními změnami, které vyžadují flexibilní správu přístupu:

- **Restrukturalizace fakult a kateder** - Možnost rychle přizpůsobit správu bezpečnostní infrastruktury organizačním změnám
- **Změny personálního obsazení IT týmů** - Snadnější předávání odpovědností při změnách v IT týmech
- **Vznik nových výzkumných center** - Možnost rychle vytvořit nový tenant pro nové výzkumné centrum
- **Změny v externích spolupracích** - Flexibilní řízení přístupu pro měnící se externí partnery

Bez multitenantního přístupu by každá organizační změna vyžadovala kompletní rekonfiguraci přístupových oprávnění a bezpečnostních politik, což by zvýšilo jak provozní náročnost, tak bezpečnostní rizika.

Závěr

Zadavatel trvá na požadavku podpory multitenantního přístupu a možnosti delegování přístupu k samostatným tenantům, protože tento požadavek je kritický pro zajištění efektivní a bezpečné správy infrastruktury vzdělávací instituce. Multitenantní přístup:

1. **Zajišťuje implementaci principu nejnižších oprávnění** - Každý administrátor má přístup pouze k té části infrastruktury, za kterou je odpovědný.
2. **Reflektuje organizační strukturu instituce** - Umožňuje delegovat správu bezpečnostních politik a konfigurací v souladu s organizační strukturou vzdělávací instituce.
3. **Zvyšuje celkovou bezpečnost** - Omezením rozsahu oprávnění snižuje potenciální dopad kompromitace administrátorských účtů.
4. **Zefektivňuje správu rozsáhlé infrastruktury** - Umožňuje paralelní práci více týmů na různých částech infrastruktury bez vzájemného ovlivňování.
5. **Umožňuje bezpečnou spolupráci s externími partnery** - Poskytuje mechanismus pro bezpečné delegování správy specifických částí infrastruktury externím dodavatelům nebo partnerským institucím.

6. **Zajišťuje soulad s bezpečnostními standardy a legislativou** - Podporuje implementaci požadavků na oddělení povinností a kontrolu přístupu dle zákona o kybernetické bezpečnosti, vyhlášky č. 82/2018 Sb. a standardů ISO/IEC 27001.

Odstranění tohoto požadavku by zásadně narušilo schopnost zadavatele implementovat potřebná bezpečnostní opatření a efektivně spravovat komplexní síťovou infrastrukturu vzdělávací instituce.

Dotaz č. 13:

Požadavek na diskové pole

Zadavatel požaduje diskové pole osazené min. 17 ks SSD SAS o kapacitě disku min. 1,92TB SSD SAS. Žádáme o vysvětlení, zda požadavek na rozšiřitelnost diskového pole pomocí expanzních jednotek) na min. 276 disků je skutečně nezbytný pro plnění účelu zakázky (zajištění kybernetické bezpečnosti) nebo zda by pro plnění účelu zakázky dané velikosti stačila nižší hodnota, např. rozšiřitelnost diskového pole pomocí expanzních jednotek) na 240 disků?

Odpověď na dotaz č. 13:

Zadavatel trvá na původním požadavku rozšiřitelnosti diskového pole pomocí expanzních jednotek na min. 276 disků. Tento požadavek je přímo spjat s cílem zakázky, kterým je zajištění kybernetické bezpečnosti, a to z následujících důvodů:

1. Legislativní opory požadavku

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

§ 4 odst. 1 - Zákon definuje bezpečnostní opatření jako "souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru."

- Požadovaná rozšiřitelnost je nezbytná pro zajištění dlouhodobé dostupnosti a spolehlivosti bezpečnostních systémů.

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních

§ 13 - Nástroje pro ochranu integrity komunikačních sítí

Povinná osoba pro ochranu integrity rozhraní vnější komunikační sítě... používá nástroje pro ochranu integrity komunikačních sítí.

- Tyto nástroje generují značné množství log souborů, které je nezbytné uchovávat pro forenzní analýzu.

§ 20 - Zaznamenávání událostí informačního a komunikačního systému

(3) Povinná osoba uchovává záznamy událostí informačního a komunikačního systému nejméně po dobu 12 měsíců.

- Tento paragraf přímo vyžaduje dostatečnou kapacitu pro uchovávání záznamů událostí po stanovenou dobu.

§ 23 - Sběr a vyhodnocování kybernetických bezpečnostních událostí

(1) Povinná osoba zajistí sběr informací o kybernetických bezpečnostních událostech a sběr provozních údajů.

- Pro splnění této povinnosti je nezbytné mít dostatečnou kapacitu úložiště pro sběr a analýzu bezpečnostních událostí.

ISO/IEC 27001:2022

Příloha A.5.33 (Záznam událostí) a **A.5.34** (Ochrana informací v protokolech) vyžaduje záznam, uchovávání a ochranu log souborů a auditních záznamů.

Směrnice NIS2 (EU) 2022/2555

Článek 21 - Opatření k řízení rizik kybernetické bezpečnosti

2. Opatření uvedená v odstavci 1 zahrnují přinejmenším: j) bezpečnost při získávání, vývoji a údržbě síťových a informačních systémů, včetně řešení a oprav zranitelností;

- Tento požadavek zahrnuje i zabezpečení dostatečné kapacity pro dlouhodobý provoz bezpečnostních systémů.

2. Konkrétní bezpečnostní důvody pro požadovanou kapacitu

2.1 Požadavky na uchovávání bezpečnostních logů

V souladu s § 20 odst. 3 Vyhlášky č. 82/2018 Sb. je povinná osoba povinna uchovávat záznamy událostí informačního systému nejméně po dobu 12 měsíců. Moderní bezpečnostní systémy generují následující objemy dat:

- **NDR (Network Detection and Response)**: 5-15 TB dat měsíčně v závislosti na velikosti sítě a hloubce inspekce
- **SIEM (Security Information and Event Management)**: 3-10 TB dat měsíčně
- **EDR (Endpoint Detection and Response)**: 2-5 TB dat měsíčně při počtu stovek zařízení

- **SOAR (Security Orchestration, Automation and Response)**: 1-3 TB dat měsíčně

Při požadavku na uchovávání dat po dobu 12 měsíců a zohlednění budoucího růstu instituce je nezbytné mít k dispozici diskové pole s dostatečnou kapacitou a rozšiřitelností.

2.2 Forenzní analýza a vyšetřování bezpečnostních incidentů

V případě bezpečnostního incidentu je kritické mít k dispozici detailní historická data o síťovém provozu a aktivitách systémů. Dle doporučení NÚKIB je pro efektivní forenzní analýzu doporučeno uchovávat:

- Raw síťový provoz (PCAP) pro klíčové segmenty sítě
- Úplné záznamy NetFlow/IPFIX
- Historické záznamy o změnách konfigurace
- Záznamy o přístupech a aktivitách uživatelů

Tyto požadavky vytvářejí potřebu významné diskové kapacity v řádu stovek TB.

2.3 Pokročilá detekce hrozeb pomocí strojového učení a umělé inteligence

Moderní systémy pro detekci hrozeb využívají metody strojového učení a umělé inteligence, které vyžadují:

- Uchovávání velkých objemů historických dat pro učení modelů
- Vytváření bezpečnostních baseline normálního chování
- Detekci anomálií na základě dlouhodobých statistik

Dostatečná rozšiřitelnost diskového pole je klíčová pro implementaci těchto pokročilých detekčních technologií.

2.4 Zálohovací a replikační strategie v kontextu kybernetické bezpečnosti

V souladu s § 13 odst. 4 Vyhlášky č. 82/2018 Sb. (dostupnost informací) je nezbytné implementovat robustní zálohovací strategii, která zahrnuje:

- Úplné zálohy všech systémů
- Inkrementální zálohy v pravidelných intervalech
- Snapshot zálohy pro rychlou obnovu
- Offline zálohy jako ochranu proti ransomware

Tyto zálohy musí být uchovávány po dostatečně dlouhou dobu, což vyžaduje významnou diskovou kapacitu.

3. Specifické důvody pro požadavek na min. 276 disků vs. 240 disků

Rozdíl mezi požadovanou kapacitou (276 disků) a navrhovanou alternativou (240 disků) představuje přibližně 13% snížení maximální rozšiřitelnosti. Toto snížení by mělo následující bezpečnostní dopady:

1. **Zkrácení doby uchovávání bezpečnostních logů** - Redukce maximální kapacity by mohla vést k nutnosti zkrátit dobu uchovávání některých typů bezpečnostních záznamů pod doporučenou hranici, což by významně omezilo možnosti zpětné analýzy při odhalení bezpečnostního incidentu.
2. **Omezení schopnosti forenzní analýzy** - Menší kapacita pro uchovávání PCAP dat a detailních síťových metadat by snížila schopnost instituce provádět důkladnou forenzní analýzu pokročilých hrozeb, které se často projevují až po delší době.
3. **Snížení odolnosti vůči ransomware útokům** - Menší kapacita pro zálohovací strategie by mohla negativně ovlivnit schopnost rychlé obnovy v případě rozsáhlého ransomware útoku.
4. **Limitovaný prostor pro bezpečnostní snímky (snapshoty)** - Snímky systémů před aplikací bezpečnostních záplat jsou kritické pro rychlý rollback v případě problémů, a jejich kapacitní omezení by zvýšilo riziko při bezpečnostních aktualizacích.

4. Závěr

Požadavek zadavatele na rozšiřitelnost diskového pole na minimálně 276 disků je plně opodstatněný z hlediska zajištění kybernetické bezpečnosti a má přímou oporu v legislativních požadavcích Zákona o kybernetické bezpečnosti, Vyhlášky č. 82/2018 Sb., standardu ISO/IEC 27001:2022 a směrnice NIS2.

Snížení tohoto požadavku by vedlo k omezení schopnosti instituce efektivně implementovat požadovaná bezpečnostní opatření, zejména v oblasti monitoringu, detekce hrozeb, forenzní analýzy a obnovy po bezpečnostních incidentech.

Zachování původního požadavku je proto nezbytné pro naplnění hlavního cíle zakázky - zajištění kybernetické bezpečnosti školské instituce.

3. Další informace

Informace 1:

Vysvětlení zadávací dokumentace je poskytováno v souladu s § 98 zákona ve lhůtě 3 pracovních dnů od doručení žádosti. Zadavatel s ohledem na obsah vysvětlení zadávací dokumentace přiměřeně prodlužuje lhůtu pro podání nabídek v souladu s § 99 zákona.

Informace 2:
Lhůta pro podání nabídek uvedená v Oznámení o zahájení zadávacího řízení se mění takto:

Lhůta pro podání nabídek – den: 06.06.2025
Lhůta pro podání nabídek – čas: 11:00

Oprava Oznámení o zahájení zadávacího řízení je zveřejněna ve Věstníku veřejných zakázek.

Aktuální lhůta pro podání nabídek je uveřejněna na profilu zadavatele.

Ve Zlíně *(dle data elektronického podpisu)*

Mgr. Filip Petráš, advokát

Digitálně podepsal Mgr. Filip Petráš, advokát
Datum: 2025.05.12 16:11:42 +02'00'

Mgr. Filip Petraš, advokát
Advokátní kancelář Petráš Rezek s.r.o.
smluvní zástupce zadavatele