

ZÁZNAM O POPTÁVKOVÉM ŘÍZENÍ

ZADAVATEL:	Západočeské muzeum v Plzni, příspěvková organizace
SÍDLO:	Kopeckého sady 357/2, 301 00 Plzeň
IČO:	00228745
ZASTOUPENÝ:	PhDr. Františkem Frýdou, ředitelem

NÁZEV VEŘEJNÉ ZAKÁZKY

„ZAJIŠTĚNÍ KYBERBEZPEČNOSTI V ZÁPADOČESKÉM MUZEU V PLZNI“

Veřejná zakázka malého rozsahu na služby zařazená do II. Skupiny Směrnice RPK č. 2/2016, o zadávání veřejných zakázek, která je mimo režim zákona č. 134/2016 Sb., o zadávání veřejných zakázek

Spisová značka:	Číslo jednací:
-----------------	----------------

Předmětem veřejné zakázky je zajistit kyberbezpečnost v Západočeském muzeu v Plzni i všech jeho pobočkách.

11x Zónový firewall se schopností hloubkové inspekce obsahu paketů „DPI“

1. POPIS PŘEDMĚTU VZ:

- Hardwarové zařízení o výšce max. 1U
- Fyzická konektivita každého zařízení min. 8x GbE, 2x SFP nebo SFP+, sériová konzole (RJ45 s příslušným převodním kabelem na RS232 nebo sériový port připojitelný pomocí micro USB)
- Všechny porty samostatně konfigurovatelné, možnost slučovat porty a jednotlivé VLAN do bridge
- Spravovatelné pomocí Web GUI, SSH, doporučeno i pomocí konzolového portu a API rozhraní z důvodu automatizace hromadných nastavení a snadné centrální správy
- Podpora bezpečnostních funkcí: DNS proxy, DNS sinkhole, ochrana před DNS rebinding, IP spoofing, TCP/UDP/ICMP flood, IP Helper min. pro DHCP (z důvodu segmentace), MAC-IP Antispoofing, audit log konfiguračních změn
- Podpora režimu DPI (hloubkové inspekce paketů) v rozsahu bezpečnostních služeb: anti-malwarová kontrola přenášených dat, IPS (detekce anomálií a signaturní detekce škodlivého kódu), filtrování obsahu (URL, kategorizace webových stránek výrobcem), řízení aplikací (povolení/zákaz/priorita, kategorizace aplikací výrobcem), schopnost kontroly i obsahu ZIP souborů, filtrování nežádoucích zemí (Geo-IP) a rizikových sítí (botnety, anonymizéry), sandbox technologie odesílající neznámé vzorky do cloudové analýzy
- Minimální propustnosti: výrobcem deklarovaná propustnost min. 2Gbps při plné hloubkové inspekci (anti-malware, IPS, aplikační kontrola), min. 500Mbps při hloubkové inspekci SSL spojení
- Podpora min. 256 VLAN
- Podpora min. 250000 souběžných spojení

- Podpora min. 128 souběžných IPSec tunelů s podporou šifrování min. AES256/SHA256 a délkou klíče min. 2048 bitů, vč. Perfect Forward Secrecy s délkou klíče min. 2048 bitů
- Spotřeba max. 200 W, možnost osazení dvěma vyměnitelnými zdroji
- Priorita: správa šířky pásma (Bandwidth Management), QoS, DCSP mapování, správa priority dle detekované aplikace
- Schopnost integrace s Active Directory, aby bylo možné na firewallu řídit přístupová oprávnění uživatelů na základě členství v AD skupinách (min. pro SPI firewall pravidla, webové kategorie a stránky, kategorie aplikací a samotné aplikace)
- Správa toků a incidentů: vizualizace toků vestavěná ve Web GUI, odesílání vybraných událostí a incidentů e-mailem, odesílání událostí vybraných na základě jejich ID protokolem syslog (z důvodu centrálního monitoringu)
- Možnost souběžné konfigurace více WAN sítí se schopností automatického přepínání mezi konektivitami na základě jejich priorit a automatické detekce funkčnosti internetu sledováním dostupnosti prostředků z každé jednotlivé WAN konektivity
- Podpora směrování: OSPF, PBR (policy based routing)
- Vizualizace realtime provozu min. na úrovni SrcIP/DstIP/Identita(uživatel)/Aplikace
- Podpora monitoringu a sledování toků: SNMP, Netflow, IPFIX
- Podpora výrobce 3 roky včetně záruky na hardware, poskytování nových firmware
- Provedení s redundantním zdrojem, včetně tohoto zdroje
- Minimálně pro 8 zařízení navíc na 3 roky podpora pravidelných aktualizací bezpečnostních služeb min. v rozsahu Gateway Antivirus a Anti-malware, IPS, URL kategorizace a filtr, botnet a Geo-IP filtr, rozpoznávání aplikací, sandbox
- Minimálně pro 1 zařízení rack-mount uchycení přímo od výrobce firewallu

1x VPN koncentrátor

- Hardware nebo virtuální appliance (pro VMware vSphere)
- Výška zařízení max. 1U (v případě fyzického HW)
- Spotřeba jednoho zařízení max. 100 W (v případě fyzického HW)
- Vzdálený přístup pomocí VPN tunelu
 - VPN navazována na protokolu SSL z důvodu snadné prostupnosti ze vzdálených sítí
 - SSL-VPN client-to-server s vlastní SSL-VPN klientskou aplikací alespoň pro platformy Mac OS, Microsoft Windows (7 a novější), Android, iOS
- Vzdálený přístup pomocí webového portálu
 - zpřístupnění vnitřních i veřejných aplikací a webů pomocí záložek, které mohou být přidělené každému uživateli zvlášť nebo pomocí členství ve skupině
 - podpora přístupu ke vzdáleným prostředkům pomocí HTML5 komponenty v prohlížeči (VNC, SSH, Terminal Services)
 - podpora přístupu ke vzdáleným prostředkům typu Terminal

Services z MS Windows 10 pomocí standardního klientského software Microsoft Terminal Services Client bez nutnosti předchozího vytvoření VPN tunelu (ke zprostředkování může být použit doplňkový software, který musí být součástí dodávky a bezplatně dostupný bez časově omezené licence)

- Reverzní proxy
 - o reverzní HTTP a HTTPS proxy
 - o možnost ověření uživatelů před povolením přístupu do webové aplikace
 - o podpora single-sign-on – pokud je uživatel ověřen na úrovni reverzní proxy, jsou jeho přístupové údaje předány do aplikace (pokud tato vyžaduje ověření pomocí Basic authentication nebo formulářového přihlášení)
 - o bez nutnosti předchozího ověření formulářovým přihlášením do reverzní proxy
- Souběžně min. 50 přihlášených uživatelů
- Autentikace a autorizace uživatelů
 - o Místní seznam uživatelů v appliance
 - o Integrace s Active Directory, LDAP, RADIUS, SAML (zejména pro integraci identit s Microsoft 365)
 - o Možnost řízení přístupů na základě skupin v AD/LDAP
 - o Možnost granulárního nastavení přístupu k jednotlivým publikovaným prostředkům každému uživateli zvlášť
- Ověřování uživatelů
 - o Dvoufaktorové ověřování (volitelné i vynutitelné)
 - o Odesílání jednorázového hesla
 - o Časově omezené heslo (Google Authenticator, Microsoft Authenticator, Duo)
- Ověřování zařízení
 - o On-boarding zařízení, ze kterého se uživatel přihlašuje
 - o Schvalování nových zařízení administrátorem
 - o Zakazování zavedených zařízení
 - o Schválení vazby uživatel/zařízení (ze schváleného zařízení se nesmí připojit kdokoli)
- Podpora výrobce min. 3 roky, řešení servisních požadavků, přístup k bezpečnostním aktualizacím, nárok na nové verze.

Implementační služby

- Revize aktuální síťové topologie, používaných VLAN, jejich zhodnocení a případný návrh nové bezpečnostní topologie podle best-practice
- Nasazení jednotlivých firewallů do infrastruktury objednatele (v místě jednotlivých lokalit – viz. níže), konfigurace VLAN včetně jejich vzájemného routingu, konfigurace pravidel, konfigurace site-to-site VPN, konfigurace bezpečnostních služeb podle požadavků objednatele
- Připojení do infrastruktury včetně zajištění potřebné kabeláže.
- Instalace a zprovoznění VPN koncentrátoru v infrastruktuře objednavatele (pro virtuální appliance možno využít VMware infrastrukturu)
- Integrace firewallů a VPN koncentrátoru s AD objednatele
- Grafická dokumentace finálního zapojení všech přístupových bodů (poboček)

	<ul style="list-style-type: none"> - Zaškolení obsluhy - Poimplementační podpora <p>Lokality pro zabezpečení firewally:</p> <ul style="list-style-type: none"> - Plzeň, Hlavní budova Kopeckého sady 2 - Plzeň, Muzeum Loutek, náměstí Republiky 23 - Plzeň, Tylova 22 - Plzeň, Zborovská 40 - Plzeň, Bolevecká náves - Plzeň, Harantova ul. - Rokycany, Masarykovo náměstí - Rokycany, nám. J. Urbana 141 (Muzeum Dr. B. Horáka) - Rokycany, Malé náměstí - Rokycany, Ulice Josefa Knihy 146 - Rokycany, Ulice Mládežníků <p>Lokality pro využití propojení prostřednictvím VPN koncentrátoru:</p> <ul style="list-style-type: none"> - Dobřív, Hamr - Zbiroh, zámek - Nepomuk, nám. Augustina Němejce 127
--	---

2. SEZNAM DORUČENÝCH NABÍDEK:

číslo	Uchazeč	Datum podání nabídky	Čas podání nabídky	Forma nabídky (elektronická / listinná)
1	business communication s. r. o. Pod Všemi svatými 15 301 00 Plzeň IČ: 26353717	29. 10. 2020	8.42 hod.	elektronická
2	IT AWACS SOLUTION s.r.o. Ocelkova 643/20 198 00 Praha 9 – Černý Most IČ: 03431045	30. 10. 2020	8.25 hod.	elektronická
3	IT FRIENDS s. r. o. U smaltovny 1381/26 170 00 Praha 7 IČ: 24656631	2. 11. 2020	9.07 hod.	elektronická

3. HODNOCENÍ:

Základním hodnotícím kritériem veřejné zakázky byla ekonomická výhodnost nabídky.

Výsledek hodnocení nabídek

číslo	Uchazeč	Celková nabídková cena v Kč bez / vč. DPH	Pořadí
1	business communication s. r. o. Pod Všemi svatými 15 301 00 Plzeň IČ: 26353717	966.693,40 Kč bez DPH/ 1.169.699,01 Kč s DPH	1.

2	IT AWACS SOLUTION s.r.o. Ocelkova 643/20 198 00 Praha 9 – Černý Most IČ: 03431045	995.600,- Kč bez DPH/ 1.204.676,- Kč s DPH	3.
3	IT FRIENDS s. r. o. U smaltovny 1381/26 170 00 Praha 7 IČ: 24656631	981.605,- Kč bez DPH/ 1.187.742,05 Kč s DPH	2.

4. VYBRANÝ UCHAZEČ:	Zadavatel vybral nabídku uchazeče business communication s. r. o., Pod Všemi svatými 15, 301 00 Plzeň, IČ: 26353717 , který splnil veškeré požadavky zadávacích podmínek, a jehož nabídka byla vyhodnocena jako cenově nejvýhodnější.
----------------------------	--

5. OSTATNÍ INFORMACE:	Záznam o poptávkovém řízení je uveřejněn na profile zadavatele v elektronickém nástroji E-ZAK: https://ezak.cnpk.cz/profile_display_....html v sekci "Veřejné dokumenty" Výzvu k podání nabídky zaslal zadavatel dodavatelům dne 22. 10. 2020 Kontrolu nabídek uchazečů provedl zadavatel s pověřenými osobami.
------------------------------	--

V Plzni dne 3. 11. 2020



Za zadavatele:

PhDr. František Frýda, ředitel

Vypracovala: Ing. Linda Trefná Kryštofová

