

Čj. MO 771194/2023-3255

Přílohy: 1

Dodatek č. 1 ke smlouvě č. 23111000469
Smlouva o poskytování služby – Školení v působnosti komunikačních a
informačních systémů XXI

uzavřený dle obecně závazných a platných právních předpisů níže uvedeného dne,
měsíce a roku, mezi těmito smluvními stranami:

I.
Smluvní strany

Česká republika – Ministerstvo obrany

Sídlo: Tychonova 221/1, 160 00 Praha 6 - Hradčany

IČ: 60162694

DIČ: CZ 60162694

Zaměstnanec pověřený jednáním: plukovník [REDACTED]

Bankovní spojení: ČNB, Na Příkopě 28, Praha 1

Číslo bankovního [REDACTED]

Kontaktní osoba ve věcech smluvních: o.z. Dana Heidenreichová, [REDACTED]

Pověřený zástupce objednatele: [REDACTED] a o.

z. Martina Rybářová, [REDACTED]

Adresa pro doručování korespondence: Agentura komunikačních a informačních systémů,

Vlastina ulice, 160 01 Praha 6 - Ruzyně

(dále jen „objednatel“)

a

GOPAS, a.s.

Obchodní společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod
sp. Značkou 7753 B

Sídlo: Kodaňská 1441/46, 101 00 Praha 10

IČ: 63911035

DIČ: CZ63911035

Její jménem jedná: Ing. [REDACTED] rady

Bankovní spojení: Raiffeisen Bank, a.s.

Číslo [REDACTED]

Kontaktní osoba: (pověřený zástupce poskytovatele) Lucie Froňková

Tel.: [REDACTED]

E-mail: [REDACTED]

Datová schránka: mi5ea5m

Adresa pro doručování korespondence: Kodaňská 1441/46, 101 00 Praha 10

(dále jen „poskytovatel“).

(objednatel a poskytovatel společně dále také „smluvní strany“ jednotlivě „smluvní strana“)

Smluvní strany se v souladu s ustanovením čl. XI. odst. 11.7 této smlouvy uzavřené dne

Agentura komunikačních a informačních systémů

Vlastina ulice, Praha 6 - Ruzyně, PSČ 160 01, datová schránka hjyaaavk

16. 5. 2023 (dále jen „smlouva“) dohodly na uzavření tohoto dodatku č. 1 (dále jen „dodatek“).

II.

Účel dodatku

1. Účelem tohoto dodatku je změna ceny za službu dle čl. IV. odst. 4.1 smlouvy a doby plnění dle v čl. V. odst. 5.1 smlouvy.

III.

Změny a doplňky

1. Text čl. IV. odst. 4.1. smlouvy se ruší a nahrazuje se textem následujícího znění:
Celková cena za službu je **1,534.486,00 Kč bez DPH a ve výši 1,856.728,06 Kč s DPH (slovy jeden milion osm set padesát šest tisíc sedm set dvacet osm korun českých šest haléřů)** (dále jen „cena“). V takto stanovené ceně jsou zahrnuty veškeré náklady poskytovatele související s plněním této smlouvy (např. DPH, zajištění prostor pro školení, materiály, clo, apod.).
2. Text čl. V. odst. 5.2 smlouvy se ruší a nahrazuje se textem následujícího znění:
Poskytovatel se zavazuje službu poskytnout **nejpozději do 24. listopadu 2023 v termínech dle smluvními stranami odsouhlaseného harmonogramu.**
3. Příloha č. 1 smlouvy se nahrazuje novou přílohou č. 1 smlouvy ve znění, které tvoří přílohu č. 1 tohoto dodatku.

IV.

Závěrečná ujednání

1. Ustanovení smlouvy včetně příloh neupravená tímto dodatkem zůstávají v platnosti beze změny.
2. Tento dodatek je vyhotoven v elektronické podobě o 2 stranách.
3. Smluvní strany prohlašují, že jim nejsou známy žádné skutečnosti, které by uzavření tohoto dodatku vylučovaly a berou na vědomí, že v plném rozsahu nesou veškeré právní důsledky plynoucí z vědomě jimi udaných nepravdivých údajů. Na důkaz svého souhlasu s obsahem tohoto dodatku připojují pod něj své podpisy.
4. Tento dodatek nabývá platnosti dnem jeho podpisu poslední smluvní stranou a účinnosti dnem jeho zveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).
5. Tento dodatek je nedílnou součástí smlouvy.

Objednatel:

plukovník Ing. Jan Jelínek

.....
ředitel

podepsáno elektronicky

Poskytovatel:

GOPAS, a.s.

Ing. Petr Daniel

.....
předseda správní rady

podepsáno elektronicky

Ing. Jan

Digitálně podepsal Ing. Jan
[podpis]

 **GOPAS**
POCITACOVA.SKOLA.CZ

Datum: 2023.11.01 11:46:45 +01'00'

Agentura komunikačních a informačních systémů

Vlastina ulice, Praha 6 - Ruzyně, PSČ 160 01, datová schránka hjyaavk

Příloha č. 1 k čj. MO 771194/2023-3255

Cenová kalkulace a specifikace služby

Podrobná specifikace a kalkulace ceny za službu - školení „Bezpečnost“

Obsah školení pro „Bezpečnost“	Nabídková cena v Kč bez DPH za 1 účastníka školení	Celkový počet účastníků	Nabídková cena v Kč bez DPH za celkový počet účastníků	Výše DPH v Kč 21% za celkový počet účastníků	Nabídková cena v Kč s DPH za celkový počet účastníků
Certified Ethical Hacker (CEHv10) (CEHv11) Obsahová náplň školení: Studenti se v rámci kurzu seznámí se strategiemi, technikami a nástroji, které se běžně používají v aktuálním hackingu a při penetračním testování. Získejte ucelený přehled technik hackingu, jako jsou pokročilá enumerace a skenování sítí či systémů v celopodnikovém rozsahu, tvorba malwaru a trojských koňů, pokročilé síťové útoky eliminující omezení VLAN a jiné techniky. Těšit se můžete na rozšířenou část testování webových serverů a aplikací, SQL Injection či hackování mobilních platform.	52.569,00	1	52.569,00	11.039,49	63.608,49
CND - Certified Network Defender Obsahová náplň školení: CND je pokročilý bezpečnostní kurz s velkým množstvím praktických ukázek a cvičení, kde si účastníci formou praktického nasazení seznámí se všemi základními komponentami obrany IT prostředí nezbytných pro efektivní obranu IT prostředí proti hackingu. Jedná se o unikátní školení, kde se každý z účastníků dozví nejčastější chyby v bezpečnosti enterprise prostředí a seznámí se s technikami zabezpečení pro eliminaci bezpečnostních rizik a tyto techniky si vyzkouší také	44.550,00	1	44.550,00	9.355,50	53.905,50

Agentura komunikačních a informačních systémů

Vlastina ulice, Praha 6 - Ruzyně, PSČ 160 01, datová schránka hjyaavk

prakticky. Je to tedy ideální školení pro budoucí IT specialisty v oboru bezpečnosti, kteří chtějí získat ucelený přehled i praktickou zkušenost IT bezpečnostních opatření.					
GOC161 – Praktická kryptografie pro správce i vývojáře Obsahová náplň školení: Kurz seznamuje posluchače praktickou cestou s principy a vlastnostmi aktuálně používaných šifrovacích a hash algoritmů, jako je AES, RSA, SHA256, SHA1, ECDSA, ECDH, RC4 a dalších, stejně jako certifikátů, PKI a protokolů vyšší úrovně jako je TLS/SSL, Kerberos, nebo DPAPI, šifrováním disků (například BitLocker) a databází, ukládáním šifrovacích klíčů a hesel na webových serverech, v databázích a prohlížečích a trezorech hesel, probírají se i časová razítka a kvalifikované zaručené certifikáty. Školení a příklady je prováděno na platformě Windows, ale všechny technologie jsou obecně platné a otevřeně standardní.	13.851,00	2	27 702,00	5.817,42	33.519,42
Network Security – Hacking v praxi (GOC3) Obsahová náplň školení: Toto školení hackingu vás seznámí se základními nástroji a principy, které se používají pro útoky a penetrační testování. Naš ojedinělý pětidenní kurz vám umožní do detailu pochopit i vyzkoušet metody, pomocí kterých se provádí útoky na počítačové sítě a serverové systémy z vnitřní části sítě a při útocih Man-in-the-Middle proti klientům mimo vnitřní síť. Účastníci si vyzkouší řadu technik jak na Windows platformě, tak i na Linuxu. Účast na tomto kurzu nebo odpovídající znalosti jsou nutným předpokladem pro účast na kurzu CEH - Certified Ethical Hacker.	27.945,00	11	307 395,00	64.552,95	371.947,95
GOC32 - Network Security - Hacking v praxi II Obsahová náplň školení:	28.350,00	10	283 500,00	59.535,00	343.035,00

Agentura komunikačních a informačních systémů

Vlastina ulice, Praha 6 - Ruzyně, PSČ 160 01, datová schránka hjyaavk

V tomto jedinečném a velmi detailním hacking kurzu přinášíme přehled útoků, které jsou pro většinu podnikových sítí nejrizikovější. Kurz vhodně rozšiřuje dlouhodobě nejoblíbenější části školení CEH a do větších detailů probírá část útoků pomocí malware a systémových útoků. Vysvětlíme si, jak často dochází k otevírání podnikové sítě na dálku pomocí malware a trojských koňů a jak lze takový útok zneužít pro kompletní ovládnutí sítě bez fyzického přístupu. V následné části systémových útoků si prokážeme, že staré zvyky správců a chyby ve správě, na kterých stále funguje většina podniků, vedou ke kompletní kompromitaci bez potřeby jakkoli prolamovat přihlašovací údaje a jak obrovsky usnadní přístup údaje získané z paměti a profilů uživatelů. Pro provedení útoků použijeme i falešná USB zařízení, která se naučíte vytvářet za běhu a pomocí kterých můžete ovládnout cizí počítač na dálku a bez vědomí uživatelů i správců jejich počítače připojit do své sítě a odcizit provoz, se kterým můžete i manipulovat. V závěrečné části kurzu se podíváme také do úvodu hackingu mobilních platforem, které lze použít jako platformu pro provedení útoku ale zacílíme si i útoky proti mobilním klientům, které vedou ke kompromitaci našich mobilních zařízení a dat na nich uložených.					
GOC33 - Network Security - Hacking v praxi III Obsahová náplň školení: V pokročilém kurzu hackingu se zabýváme pokročilými síťovými útoky pro detailní průzkum síťového prostředí. Naučíme se zneužívat slabiny v chybné implementaci zabezpečení ethernet i WiFi sítí. Vyzkoušíme si přístup ochranou sítě na úrovni L2 v podobě VLAN hoppingu i L3 v podobě útoků na routery. Seznámíte se do detailu s možnostmi skenování cílů a to i v situaci, kdy nemáte možnost skenovat cíle napřímo. Seznámíme se s principy nejčastějších webových útoků, které si	28.350,00	5	141 750,00	29.767,50	171.517,50

Agentura komunikačních a informačních systémů

Vlastina ulice, Praha 6 - Ruzyně, PSČ 160 01, datová schránka hjyaavk

vyzkoušíme prakticky proti klientům i serverům. Účastníci se seznámí se zneužíváním útoků XSS, Cross Site Request Forgery, SQL injection, blind SQL injection, command injection a dalších. Seznámíme se i s hackingem bezdrátové komunikace pomocí Software Defined Radio a hackingu BluetoothLE. V další části pak využíváme předešlé získané znalosti k analýze a útokům na IoT zařízení, ovládání kamery, žárovky nebo embeded zařízení, takže si ukážeme i hacking HW.					
Webhacking v praxi – Zranitelnost webových aplikací (GOC54) Obsahová náplň školení: Toto školení vás zasvěťí do tajů webhackingu a zranitelností webových aplikací, které umožňují útočit na koncové uživatele služby. Školení Vám umožní do detailu pochopit a v praxi si vyzkoušet metody, které běžně používají útočníci. Zranitelnosti webových aplikací umožňující útoky na koncové uživatele patří mezi nejčastější typy webových zranitelností a důkladně by s nimi proto měli být seznámeni všichni vývojáři a provozovatelé webových aplikací. Přestože to nemusí být na první pohled zřejmé, mohou mít tyto útoky velice vážné dopady včetně kompletního převzetí kontroly nad cílovým systémem. Seznamte se s těmito zranitelnostmi a otestujte si bezpečnost svých webových aplikací dříve, než to za vás udělá nevídaný vetřelec.	25.110,00	3	75 330,00	15.819,30	91.149,30
GOC55 - Testování bezpečnosti webových aplikací Obsahová náplň školení: Na kurzu se dozvíte kdy a jak webovou aplikaci efektivně testovat. Naučíte se, jak provádět manuální i automatické testy bezpečnosti a jak vhodně jednotlivé testovací metody kombinovat. Seznámíte se s projektem OWASP, s jeho metodikami a volně dostupnými nástroji. Po absolvování	25.110,00	2	50 220,00	10.546,20	60.766,20

Agentura komunikačních a informačních systémů

Vlastina ulice, Praha 6 - Ruzyně, PSČ 160 01, datová schránka hjyaavk

kurzu budete schopni provést samostatně penetrační testy webové aplikace, správně ohodnotit rizika spojená s nalezenými zranitelnostmi, a vystavit závěrečnou zprávu s výsledky bezpečnostního testu. Mimo to se naučíte, jak vhodně evidovat a revidovat bezpečnostní nálezy a jak měřit přínosy zavedení bezpečnostního testování.					
GOC56 - Bezpečnost a hacking Android aplikací Obsahová náplň školení: Toto školení vás zavede do tajů hackování na platformě Android. Umožní vám do detailu pochopit a vyzkoušet si metody, pomocí kterých se provádí útoky na mobilní aplikace. V průběhu kurzu si postupně vysvětlíme i vyzkoušíme vše, co potřebujete znát pro obranu proti technikám útoků zneužívajících zranitelnosti mobilních aplikací, jež mohou vést k úniku důvěrných dat, k obejití autentizace, nebo dokonce k plnému ovládnutí mobilního zařízení. Tento kurz vás naučí jak si otestovat bezpečnost svých aplikací dříve, než to za vás udělá někdo jiný s nekalými úmysly.	25.110,00	3	75 330,00	15.819,30	91.149,30
Checkpoint certified security administrator gopas (CCSAR80) Obsahová náplň školení: Kurz obsahuje vše, co potřebujete ke spuštění, konfiguraci a správě každodenního provozu bezpečnostní brány Check Point a Management serveru R81.10 na operačním systému GAI. Naučíte se s námi základní koncepty a získáte znalosti potřebné pro správu bezpečnostního řešení Check Point.	31.490,00	1	31 490,00	6.612,90	38.102,90
Checkpoint security expert (CCSER80) Obsahová náplň školení: Na tomto pokročilém kurzu si rozšíříte znalosti jak instalovat a upgradovat bezpečnostní systémy GAI. Získáte přehled o procesech a možnostech řešení problémů. Díky praktickým labům si vyzkoušíte upgrade brány	34.310,00	1	34 310,00	7.205,10	41.515,10

Agentura komunikačních a informačních systémů

Vlastina ulice, Praha 6 - Ruzyně, PSČ 160 01, datová schránka hjyaavk

i management serveru. Teorie se zabývá možnostmi VPN, ClusterXL, API a akceleračními technikami. S námi si ověříte a rozšíříte své znalosti pro správu pokročilého zabezpečení systému Check Point.					
Palo Alto Firewall 9.0 Essentials: Configuration and management (EDU-210) Obsahová náplň školení: Kurz zlepší porozumění studentům, jak nakonfigurovat a spravovat brány firewall nové generace Palo Alto Networks. Kurz zahrnuje praktické zkušenosti s konfigurací, správou a monitorováním firewallu v laboratorním prostředí.	54.460,00	4	217 840,00	45 746,40	263.586,40
McAfee ePolicy Orchestrator a Endpoint Threat Protection (fa Comguard) Obsahová náplň školení: Kurz poskytne komplexní informace a praktické zkušenosti s instalací, správou a pokročilými nastaveními. Poskytne odpovědi na nejčastěji řešené situace při implementaci do LAN / WAN.	17.500,00	11	192 500,00	40.425,00	232.925,00

Celková cena* za školení „Bezpečnost“ a daný počet všech účastníků v Kč bez DPH	1.534.486,00
Výše DPH v Kč 21%	322.242,06
Celková cena* za školení „Bezpečnost“ a daný počet všech účastníků v Kč s DPH 21%	1.856.728,06

* Celková cena zahrnuje veškeré náklady související s plněním veřejné zakázky (zejména zajištění prostor, materiály a ostatní náležitosti k tíži poskytovatele související s poskytnutím služby).

