OBJEDNÁVKA

Objednavatel

Státní investiční a rozvojová společnost, a.s.
zapsaná v OR: Městský soud v Praze, sp. zn. B 28761
se sídlem: Na Poříčí 1046/24, Nové Město, 110 00 Praha 1
[redacted]
IČO: 21333858, DIČ: CZ21333858

Dodavatel

Trusted Network Solutions, a.s.
zapsaná v OR: Krajský soud v Brně, sp. Zn. B 8966
se sídlem: Ptašínského 309/6, 602 00 Brno
IČO: 21771189
DIČ: CZ21771189

Předmět, termín a místo plnění

Objednáváme provedení penetračního testu webové aplikace dle vaší nabídky viz příloha této Objednávky.
Výše uvedené služby budou dodány v termínu do sedmi pracovních dnů od písemné výzvy k započetí penetračního testování.
Místo plnění je sídlo objednatele

Cena

Celková cena: 88.200,- Kč bez DPH:

Platební podmínky

Objednatel uhradí cenu na základě faktury, kterou dodavatel vystaví a zašle na e-mailovou adresu: [redacted] objednateli nejpozději do 10 (slovy: „deseti“) kalendářních dní po řádném plnění této objednávky, což bude stvrzeno podepsáním Akceptačního protokolu.
Příslušnou cenu uhradí objednatel formou bezhotovostního převodu na účet dodavatele uveden na faktuře. Faktura musí obsahovat odkaz na tuto Objednávku. Dále musí každá faktura obsahovat veškeré náležitosti daňového dokladu stanovené příslušnými právními předpisy, zejména zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a § 435 občanského zákoníku.
Splatnost faktury činí 30 (slovy: „třicet“) kalendářních dní a počítá se ode dne doručení faktury objednateli.

Nebude-li faktura splňovat veškeré výše uvedené náležitosti daňového dokladu, nebo bude-li mít jiné závady v obsahu, je objednatel oprávněn ji ve lhůtě její splatnosti dodavateli vrátit a dodavatel je povinen vystavit a doručit objednateli fakturu opravenou či doplněnou. V případě vrácení faktury dle předcházející věty se lhůta splatnosti přerušuje a nová lhůta splatnosti počíná běžet od počátku až dnem následujícím po dni, kdy byla opravená nebo doplněná faktura splňující všechny náležitosti dle příslušných právních předpisů a požadavky dle této smlouvy, doručena objednateli.

Smluvní pokuty

Při nedodržení výše stanoveného termínu dodání předmětu plnění Vám bude účtována smluvní pokuta ve výši 0,05% z ceny plnění za každý i započatý den prodlení.

Ostatní ujednání

Akceptací této objednávky dodavatel souhlasí se zveřejněním celého obsahu objednávky v registru smluv pro případ, že podléhá povinnosti zveřejnění ve smyslu zákona č. 340/2015 Sb., o registru smluv, a prohlašuje, že objednávka neobsahuje obchodní tajemství ani údaje, které by neměly být zveřejněny, s výjimkou údajů, které dle názoru objednatele naplňují výjimku z povinnosti zveřejnění dle zákona o registru smluv. Pro případ, že by dodavatel zjistil, že objednávka obsahuje obchodní tajemství popř. údaje, které dle právních předpisů nemají být zveřejněny, zavazuje se do tří dnů od obdržení objednávky předat objednateli kopii objednávky se začerněnými údaji, které nemají být zveřejněny, a s poskytnutím odůvodněním pro jejich nezveřejnění.

Přílohy:

a) Nabídka ze dne 20.09.2024 platná do 30.11.2024

[redacted] ta el. podpisu

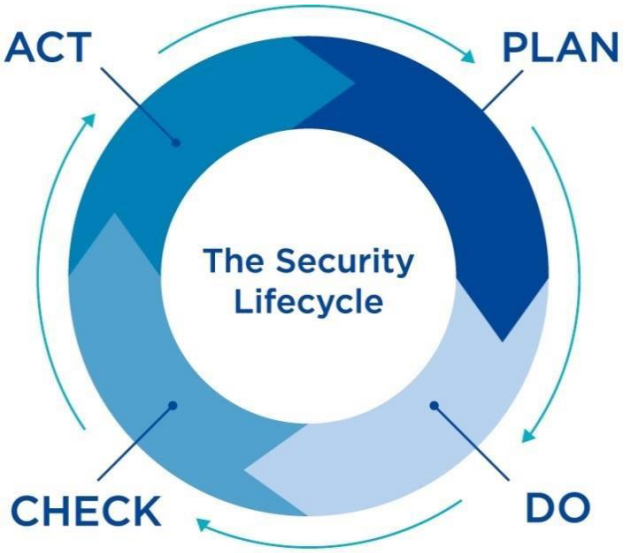
[redacted]

Ing. Petr Križan
místopředseda představenstva

[redacted]

Ing. David Petr
člen představenstva

TRUSTED
NETWORK
SOLUTIONS



Nabídka

Penetrační testy webové aplikace

Zadavatel	**Státní investiční a rozvojová společnost, a.s.**
Datum vytvoření	20.9.2024
Platnost nabídky	30.11.2024
Číslo nabídky	24-461
Klasifikace	Interní dokument

Obsah nabídky

Základní informace o dodavateli

Obchodní jméno	Trusted Network Solutions, a.s.
Sídlo společnosti	Ptašínského 309/6 602 00 Brno Česká republika
Právní forma	Akciová společnost IČO: 21771189 DIČ: CZ21771189 Společnost zapsána v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl B, vložka 8966
Vedení společnosti	[redacted]
Bankovní spojení	[redacted]
ID datové schránky	6rdv4yx
Datum vzniku	1. července 2024
Vytvořil	[redacted]
Web	www.tns.cz

20.9.2024

Libor Havelka

Nabídka

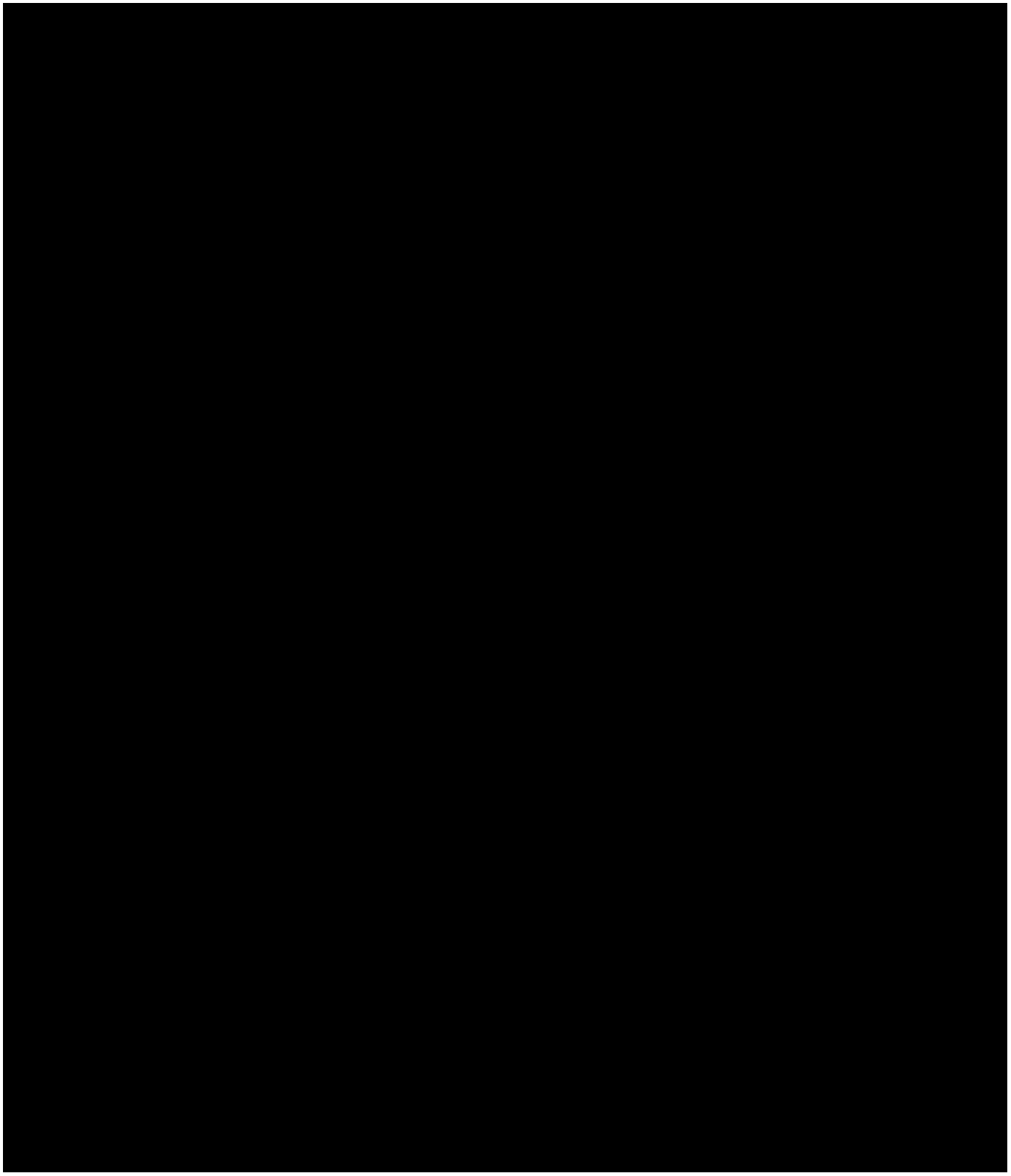
Na základě průzkumu trhu **společnosti Státní investiční a rozvojová společnost, a.s.** na provedení penetračního testu webové aplikace vám předkládáme nabídku našich služeb.

Cílem testování je ověřit zabezpečení a identifikovat zranitelností webové aplikace v organizaci proti potenciálním útokům a hrozbám. Testování bude probíhat po vzájemné dohodě se zadavatelem, jako nedestruktivní a neinvazivní testování ve vybraném termínu, časových rámcích a v definovaných lokalitách. Zranitelnosti mohou být prozkoumány až na úroveň identifikace konkrétních exploitů, nicméně jejich použití, které by mohlo narušit důvěrnost, integritu či dostupnost systémů bude vždy konzultováno se zadavatelem. Jednotlivé fáze testování jsou popsány v popisu a harmonogramu projektu.

Nabídka obsahuje popis metodiky a postupů dodavatele, detailní popis jednotlivých poptávaných služeb, představuje realizační tým a harmonogram projektu včetně cenové kalkulace. Součástí nabídky jsou také vybrané reference úspěšně realizovaných projektů.

Nabídka vychází z kvalifikovaného odhadu předpokládaného rozsahu práce a může být dle specifických požadavků zadavatele dále upravena.

Metodika a obecný postup



Metodika a standardy

[redacted]

Postup testování

Samotné testování se skládá ze šesti etap s různou mírou vyžadované součinnosti zákazníka. Doporučenou 7. etapou pak může být re-test sloužící k ověření přijatých opatření.

1.) Sběr informací

V první fázi je pozornost zaměřena na získávání informací, podle kterých budou v následujících fázích definovány testovací scénáře proveditelné u zadavatele. Pozornost je zaměřena primárně na hardwarová a softwarová aktiva, případně také na lidské zdroje, které by mohly být během testu využity k úspěšnému narušení bezpečnosti. Tato fáze zahrnuje především aktivní skenování sítě, serverů a dalších aktivních prvků a detekci používaných služeb.

2.) Hodnocení aktiv a identifikace cílů

Druhá fáze je zaměřena na ohodnocení aktiv dle typu OS/firmware, citlivosti uložených dat, otevřených portů a podobně. Kritickým aktivům je přiřazena nejvyšší priorita pro testování. Z takto ohodnocených aktiv jsou identifikované potenciální cíle a scénáře pro penetrační testy.

3.) Identifikace zranitelností

Proces identifikace zranitelností spočívá v objevování slabých míst v aktivech – konkrétních systémech, které mohu být využity pro narušení bezpečnosti zadavatele (např. ve formě průniku, nedostupnosti služeb, neoprávněnému zpřístupnění – pozměnění dat). Způsob identifikace zranitelností je závislý na použitých technologiích a zjištěných informacích. V této fázi jsou typicky používány automatizované nástroje pro nalezení známých zranitelností. Speciální pozornost je pak věnována nesprávné konfiguraci např. nezabezpečenému přenosu citlivých informací či použití slabých šifrovacích a autentizačních schémat.

4.) Verifikace zranitelností a pokus o narušení bezpečnosti

Pokus o narušení bezpečnosti představuje snahu o využití nalezených zranitelností pro neautorizovaný přístup, eskalaci uživatelských privilegií, znepřístupnění služby a další nepřátelské akce vůči systémům zadavatele. Při průniku se postupuje s nejvyšší obezřetností, aby nedošlo k poškození anebo znehodnocení testovaných služeb. Cílem všech uskutečněných testů je ověření nalezených zranitelností spolu s individuálními chybami nenalezenými pomocí automatizovaných nástrojů.

5.) Identifikace dopadů po zneužití zranitelnosti

Po úspěšném narušení bezpečnosti je potřebné přezkoumat dostupná data, oprávnění a možnosti dalšího zneužití potenciálním útočníkem. Na konci této fáze dochází k odstranění všech testovacích účtů pořízených pro potřeby testování a také škodlivého, případně nestandardního zdrojového kódu, zaslaného na testované služby.

6.) Tvorba závěrečné zprávy

Závěrečná zpráva včetně manažerského shrnutí obsahuje detailní popis testování, sumarizaci nalezených zranitelností a bezpečnostních mezer, ohodnocení jejich závažnosti, dopadů a rizik. Definuje doporučení k eliminaci zranitelností a minimalizaci rizik.

7.) Re-test

Po eliminaci zranitelností a přijetí dalších opatření pro minimalizaci rizik spojených s potenciálním útokem je doporučeno uskutečnit re-test. Ten slouží k potvrzení správné implementace nápravných opatření a případně identifikaci nových zranitelností, které mohly být do systému zaneseny při realizaci nápravných opatření.

Portfolio penetračních testů

Síťová bezpečnost

- Externí penetrační test infrastruktury
- Interní penetrační test infrastruktury
- Penetrační test bezdrátových sítí
- Audit OS/DBMS/SaaS platforem

Aplikační bezpečnost

- Penetrační test webové aplikace a související infrastruktury
- Penetrační test desktop aplikace
- Penetrační test mobilní aplikace

Sociální inženýrství

- E-mailový test – Phishing
- Telefonický test – Vishing
- Cílený test – Spear phishing
- Aktivní test fyzické bezpečnosti
- Pasivní test fyzické bezpečnosti

Specializované služby

- Red teaming
- Simulace odcizení zařízení
- Zátěžový test – DoS
- Analýza otevřených zdrojů – OSINT
- Cvičení kybernetické bezpečnosti
- Školení zaměstnanců

Realizační tým

[redacted]

Popis projektu

Penetrační test webové aplikace a související infrastruktury

Cílem penetračního testu webové aplikace a souvisejících služeb je nestandardními akcemi uživatele demonstrovat zranitelnosti, kterými je možno realizovat průnik do interní infrastruktury zadavatele nebo získat citlivá data či upozornit na chyby v aplikační logice testované aplikace. Test je prováděn v režimu black-box, tj. pouze se znalostí webové adresy aplikace, ale i v režimech grey-box a white-box, kdy má auditor autentizovaný přístup k aplikaci a případně také informace o vnitřním fungování aplikace. Realizovány jsou jednak automatizované testy zranitelností, tak i manuální testy dle standardu OWASP a interních postupů s využitím specializovaných nástrojů.

V rámci testu jsou realizovány následující činnosti:

- Kontrola nastavení bezpečné komunikace (např. parametry SSL/TLS šifrování).
- Náchylnost k DoS/DDoS útokům.
- Chyby aplikační logiky (výpočty, náhodné chyby, ztráta dat).
- Možnost zneužití aplikace neautorizovaným způsobem – chyby v autentizaci, XSS, SQL Injection.
- Zneužití komponent se známými zranitelnostmi.
- Získaní citlivých informací z testované aplikace.
- Pokus o získání přihlašovacích údajů registrovaného uživatele.
- Testy podpůrné infrastruktury webové aplikace (např. API, backend systémy a databáze) a jejich bezpečná integrace v rámci testované aplikace.
- Návrh nápravných opatření a tvorba závěrečné zprávy.

Harmonogram projektu

		Časový rámec (man-day)	
		Dodavatel	Zákazník
Etapa 1 - Zahájení projektu		**0,3**	**0,5**
1	Kick-Off projektu - upřesnění kontaktních a pohotovostních kontaktů, upřesnění zadání a cílů projektu, upřesnění výstupů projektu, identifikace možných rizik	0,3	0,5
Poznámky:			
Etapa 2 - Penetrační test webové aplikace		**5,0**	**1,1**
Část 1 - Identifikace zranitelností automatizovanými nástroji		1,0	0,6
1	Sběr informací a identifikace zranitelných cílů	0,5	0,3
2	Identifikace zranitelností automatizovanými nástroji	0,5	0,3
Část 2 - Podrobná verifikace zranitelností ručními postupy		4,0	0,5
1	Verifikace zranitelností specializovanými nástroji a manuálními postupy	1,0	0,3
2	Další pokusy o narušení bezpečnosti	2,5	0,2
3	Vyhodnocení a dokumentace nálezů	0,5	-
Etapa 3 - Vyhodnocení a akceptace		**1,0**	**1,0**
1	Tvorba a předání závěrečné zprávy	0,7	0,5
2	Zapracování připomínek, akceptace projektu	0,3	0,5
Předání výstupů zadavateli, zpracování zaslaných připomínek a akceptace celého projektu zadavatelem.			

Celkem	**6,3**	**2,6**

Cenová kalkulace

	Časový rámec man-day	Cena 1 man-day	Cena
Etapa 1: Zahájení projektu Vstupní dokumentace a přípravné práce	[redacted]	[redacted]	[redacted]
Etapa 2: Penetrační test webové aplikace	[redacted]	[redacted]	[redacted]
Etapa 3: Vyhodnocení a akceptace Závěrečná zpráva, návrh doporučení, akceptace a předání projektu	[redacted]	[redacted]	[redacted]
Celkem	[redacted]	–	[redacted]
CENA PROJEKTU	**88 200 Kč**		

Ceny jsou uváděny bez DPH 21 %

Reference

Kooperativa pojišťovna
Vienna Insurance Group

Penetrační testy infrastruktury sítě, Penetrační testy aplikací, Penetrační testy webových služeb, Audit koncových stanic, Penetrační test sociálním inženýrstvím.

Banka CREDITAS

Penetrační test internetového bankovnictví,
Test zranitelností interní sítě, Audity konfigurace, Penetrační testy mobilních a webových aplikací.

PPF banka

Penetrační test internetového bankovnictví včetně testu mobilních aplikací a následný kontrolní Re-test. Penetrační test odolnosti uživatelů – phishing.

Generali Investments CEE, investiční společnost

Penetrační testy tří vybraných webových aplikací v testovacím i produkčním prostředí.

Úřad pro ochranu hospodářské soutěže

Externí a interní penetrační testy infrastruktury,
Penetrační test webové aplikace, Testy odolnosti uživatelů metodami sociálního inženýrství, Re-test.

Canadian Medical

Penetrační testy čtyř vybraných webových a desktop aplikací.

MND Energie

Interní penetrační testy – prověření odolnosti informačních systémů vůči potenciálním útokům z prostředí vnitřní sítě.

Český hydrometeorologický ústav

Penetrační testy webových aplikací a služeb.

Povodí Odry, státní podnik

Externí penetrační test zahrnující test webových aplikací, Interní penetrační test zahrnující test informačních systémů, Penetrační test Wi-Fi sítě. Testy odolnosti uživatelů vůči kybernetickým útokům metodami sociálního inženýrství.

ČEVAK

Penetrační testy odolnosti uživatelů formou phishingu a školení uživatelů. Zajištění souladu a vypracování dokumentace ke kybernetické bezpečnosti. Externí výkon funkce manažera kybernetické bezpečnosti.

Kraj Vysočina

Bezpečnostní a penetrační testy, Penetrační testy formou sociálního inženýrství s cílem prověření a zmapování úrovně informační a kybernetické bezpečnosti v personální oblasti.

Jihočeská univerzita v Českých Budějovicích

Penetrační testy odolnosti uživatelů formou sociálního inženýrství, zaměřeny na praktické testování uživatelů a jejich povědomí o informační bezpečnosti – phishing, vishing, pasivní i aktivní test fyzické bezpečnosti.

Psychiatrická nemocnice v Opavě

Externí a interní penetrační test infrastruktury,
Penetrační test Wi-Fi sítě.

Global Payments Europe

Penetrační testy mobilních aplikací a API.

Dopravní podnik Ostrava

Externí penetrační test zahrnující test webových aplikací,
Interní penetrační test zahrnující test informačních systémů,
Testy odolnosti uživatelů metodami sociálního inženýrství,
Penetrační test Wi-Fi sítě.

Státní veterinární ústav Jihlava

Penetrační testy infrastruktury sítě, Testy bezdrátových sítí,

.

Ministerstvo životního prostředí

Penetrační test webové aplikace, Penetrační test interního systému, Penetrační test informačního systému.

Letiště Praha

Penetrační test webové aplikace.

TŘINECKÉ ŽELEZÁRNY

Penetrační testy infrastruktury, Externí penetrační test.

TESCOMA

Penetrační testy a test zranitelností e-shopu.

M&M reality holding

Analýza současného stavu plnění GDPR a revize dokumentů.

O nás

Společnost Trusted Network Solutions patří mezi přední české IT společnosti s mnohaletými zkušenostmi v oblasti informační a kybernetické bezpečnosti. Dlouhodobě se věnujeme ochraně dat a informací, které jsou dnes jedním z nejvýznamnějších aktiv každé organizace. Poskytujeme odborné konzultační služby zaměřené na penetrační testování a systematické řízení informační a organizační bezpečnosti.

Využijte naši odbornost a zkušenosti

- Penetrační testy, Technické a zátěžové testy
- Audit zabezpečení informačních systémů, aplikací a služeb
- Analýza současného stavu, Analýza rizik
- Návrh a formulace nápravných opatření
- Řízení bezpečnosti, Řízení kontinuity činností
- Bezpečnostní manažer, Pověřenec pro ochranu osobních údajů
- Legislativa GDPR, ISMS, ISVS, Kybernetický zákon, Utajované informace
- Školení bezpečnosti, Příprava na certifikaci

Více informací o našich poskytovaných službách a řešeních:

tns TRUSTED NETWORK SOLUTIONS

www.tns.cz