Specifikace předmětu plnění

technické podmínky

# Bezpečný DNS systém

Předmětem veřejné zakázky je nasazení systému pro komplexní zabezpečení DNS (Domain Name System) provozu zadavatele (dále jen systém), které bude sestávat z:

* dodání systému,
* implementace včetně základní konfigurace,
* provedení školení a
* zpracování bezpečnostně-provozní dokumentace,

a to dle níže uvedených požadavků.

Systém musí sloužit pro:

* bezpečný překlad externích domén;
* správu, řízení, monitoring a analýzu DNS provozu;
* detekci a případnou blokaci anomálií v DNS provozu;
* detekci a blokaci hrozeb určených na základě různých zdrojů tzv. threat intelligence;
* ochranu před minimálně těmito hrozbami:
  + známé hrozby dle threat intelligence,
  + zero-day hrozby využívající DGA,
  + DNS tunneling,
  + cílený phishingový útok,
  + phishingový homografový útok (nepovinný požadavek, kvalitativní výhoda).

Systém musí být odolný proti zneužívání zranitelností v DNS provozu.

## Požadavky na funkcionalitu systému

Systém jako celek musí podporovat tuto funkcionalitu:

* monitoring DNS dotazů – tedy příjem, zpracování, ukládání a vyhodnocování logů (auditních záznamů) o provedených DNS dotazech,
* vyhodnocování DNS dotazů na základě
  + threat intelligence databáze,
  + uživatelsky definovaných allow (white) a deny (black) listů
  + behaviorální analýzy za účelem ochrany před hrozbami typu:
    - DNS tunneling,
    - zero day útok využívající DGA,
    - cílený phishingový útok,
    - phishingový homografový útok (nepovinný požadavek, kvalitativní výhoda)
* nastavení 2 úrovní fungování:
  + blokování všech škodlivých DNS dotazů a
  + auditing (bez blokování) všech škodlivých DNS dotazů
* třetí úroveň fungování – blokování a auditing na základě politik (např. dle score nebo typu hrozby v ThreatIntelligence databázi) – (nepovinný požadavek, kvalitativní výhoda)
* agent nastavuje DNS server pro všechna relevantní síťová rozhraní klienta a to tak, že automaticky rozpoznává umístění klienta v síti, přičemž zohledňuje model nastavení, kdy
  + zůstávají funkční stávající lokální DNS resolvery v LAN síti pro překlad interních domén,
  + zůstává zachována funkcionalita obecných hotspotových systémů s captive portály
  + a zůstává zachován účel bezpečného překlad externích domén pomocí systému
* chování agenta může být založeno např. na principu zjišťování dostupnosti bezpečných DNS resolverů z lokální sítě
* agent umožňuje nastavení zajištění ochrany proti odchytávání DNS dotazů přes transparentní DNS proxy poskytovatele konektivity cizí sítě pomocí DNSoverTLS a to pouze oportunistickým způsobem (nepovinný požadavek, kvalitativní výhoda)

## Požadavky na součásti systému

Systém musí obsahovat níže uvedené součásti s níže uvedenými vlastnostmi.

### DNS resolver

DNS rekurzivní resolver musí splňovat tyto požadavky:

* implementace v HA režimu formou technologie anycast, kdy minimálně jeden node je umístěn v prostředí zadavatele, tzv. on-premise
* on-premise node bude dodán buď jako samostatný HW box nebo formou virtuální appliance do virtualizační platformy VMware (VMware vSphere Enterprise verze 8+); pro tyto účely zadavatel poskytne virtuální stroj s těmito parametry:
  + 8 CPU COREs
  + 16 GB RAM
  + Max. 100 GB HDD
  + OS dle volby dodavatele (v případě licencovaného OS všechny potřebné licence zajistí dodavatel)
* správa všech nodů DNS resolverů (včetně OS) bude plně v režii dodavatele
* dostupnost nodů na veřejně dostupné IP adrese
* podpora protokolů IPv4 a IPv6
* podpora DNSSEC

### Administrační portál

Administrační portál musí být implementovaný jako webová aplikace přístupná pomocí tenkého klienta (browseru) a musí obsahovat minimálně následující vlastnosti:

* funkce zobrazování DNS statistik
  + souhrnné statistiky DNS provozu
* funkce zobrazování DNS logů (všech DNS dotazů), a to pouze legitimních uživatelů služby (tedy z definovaných sítí zadavatele a zařízení s instalovanými agenty)
  + zobrazení formou tabulky
  + položky logu/záznamu
    - datum a čas
    - IP klienta
      * Pokud je klient lokální - IP samotného klienta
      * Pokud je klient v páteřní síti zadavatele Rowanet - veřejná adresa koncové sítě (MAN sítě umístěné v MPLS páteřní síti)
      * Pokud je klient v Internetu (na klientovi je nainstalovaný agent) – veřejná IP adresa poskytovatele connectivity
    - Název klienta – pouze v případě instalovaného agenta
    - Typ dotazu
    - Obsah dotazu
    - Doména 2. řáduz DNS dotazu (např. ve tvaru domena\_druheho\_radu.tld)
    - Odpověď (DNS response)
  + funkce filtrování dle jednotlivých položek
  + funkce zobrazení záznamů v grafu (reagujícím na filtry) - např. časové osy, apod.
* funkce zobrazování DNS hrozeb
  + stejné jako zobrazování DNS logů v tabulce s tím, že focus/filtr bude zaměřen na vyhodnocené hrozby
  + zobrazení příznaku zda bylo povoleno|auditováno|blokováno (podle nastavené politiky)
* funkce passiveDNS – zobrazení historie DNS jmen a jejich IP adres
* funkce zobrazení přehledu zařízení s instalovaným agentem
  + aktuální IP adresa + historie přidělených IP adres
  + Název zařízení
  + Poslední kontakt
  + Verze agenta
  + Verze operačního systému
* funkce konfigurace uživatelů portálu a jejich oprávnění
* portál umožňuje autentizaci pomocí SAML2 protokolu vůči IDP zadavatele (postavený na technologii Shibboleth, vysocinaid.kr-vysocina.cz) (nepovinný požadavek, kvalitativní výhoda)
* Exporty vybraných DNS dotazů/logů (CSV)
* Možnost konfigurace „pseudo“ tenantního přístupu k DNS logům
  + Např. pomocí vytvoření uživatele portálu a přiřazení oprávnění k prohlížení záznamů pro vybrané IP prefixy, nebo jiným, vhodným způsobem tak, aby byla dodržena zmíněná logika
* Možnost konfigurace „pseudo“ tenantního přístupu k přehledu a správě zařízení s instalovaným agentem

Nepovinné požadavky, jejichž splnění představuje kvalitativní výhodu ve výběrovém řízení:

* Možnost zobrazení přehledu resolverů (servery, IP adresy, jejich stav)
* Definice politik překladů a blokování (např. dle skóre nebo míry reputace v ThreatIntelligence databázi)

### Agent (klientská služba)

Agent bude sloužit pro zajištění DNS překladu prostřednictvím systému v případech, kdy klient (mobilní zařízení zadavatele) bude mimo LAN a mimo páteřní síť zadavatele. Agent musí splňovat následující vlastnosti a funkcionalitu:

* agent musí být instalovatelný na mobilní zařízení s operačními systémy MS Windows (10 a 11), OS Android 8 a vyšší a IOS 12 a vyšší
  + u OS Android a IOS možnost instalace z Google Play a App Store včetně mechanizmu zajištění autenticity klienta (kdy nesmí být možné instalovat klienty a tak využívat celý systém neoprávněným uživatelem, jiným subjektem či veřejností)
  + aktualizace agenta pro OS Android a IOS je prováděna prostřednictvím Google Play a App Store
* aktualizace agenta pro MS Windows musí probíhat automaticky
* provozovatelem a publikátorem aplikace/agenta v Google Play a App Store bude přímo dodavatel systému
* agent musí umožňovat hybridní model deploymentu pro MS Windows prostředí – automatický i ruční
* v rámci deploymentu agenta musí dojít k nějaké formě ověření (autentizace či autorizace) uživatele/zařízení, aby bylo zabráněno využívání aplikace neoprávněnými uživateli

### Threat Intelligence databáze

Threat Intelligence databáze bude součástí systému a bude zajišťovat zdroje informací pro vyhodnocování hrozeb uvedených ve funkčních požadavcích. Systém musí obsahovat povinně minimálně 3 zdroje pro Threat Intelligence, a to:

* 1 komerční databázi poskytovanou buď přímo dodavatelem nebo třetí stranou (licence pro použití této datáze bude již zahrnuta do celkové ceny systému)
* databázi, která je součástí projektu Warden/NERD sdružení CESNET (<https://warden.cesnet.cz/>, https://nerd.cesnet.cz)
* zákony stanovené blacklisty pro poskytovatele připojení v České republice, jako např.
  + seznam stránek s nelegální nabídkou léčivých přípravků (dle zákona č. 378/2007 Sb., o léčivech
  + seznam nepovolených internetových her (dle zákon č. 186/2016 Sb. o hazardních hrách)

Systém dále musí umožnit případné připojení další databáze vybrané zadavatelem. Tato databáze není součástí dodávky v rámci veřejné zakázky, licenční práva k databázi půjdou na vrub zadavatele a technické připojení této DB bude řešeno v rámci servisu dle platného servisního smluvního vztahu s dodavatelem.

## Licenční požadavky

* Dodaný systém nesmí z licenčního hlediska omezovat množství uživatelů a zařízení (nepovinný požadavek, kvalitativní výhoda)
* Pokud bude systém licenčně omezovat použití množství uživatelů a zařízení, musí být dodány takové licence, které umožní použití pro minimálně:
  + 1000 uživatelů ve vnitřní síti zadavatele,
  + 2000 zařízení (pracovní stanice, mobilní zařízení i servery) ve vnitřní síti zadavatele,
  + 1000 zadavatelem vlastněných zařízení mimo vnitřní síť (pro účely instalace agenta),
  + 15 000 uživatelů, kteří jsou umístěni v koncových sítích připojených k páteřní síti zadavatele (Rowanet) a pro zadavatele jsou tudíž anonymní (zadavatel v tomto případě vystupuje v roli ISP),
  + pro 15 000 zařízení anonymních uživatelů mimo páteřní síť (pro účely instalace klientské služby) – jedná se o uživatele organizací připojených do páteřní sítě zadavatele (Rowanet),
  + pro 150 organizací připojených do páteřní sítě zadavatele,
  + neomezený počet administrátorů přistupujících do webového portálu.
* Přičemž zadavatel požaduje poskytnutí takové licence včetně 5 leté podpory (nároky na dodání bezpečnostních a dalších aktualizací a aktualizací threat intelligence databáze) a to za účelem udržitelného a hlavně bezpečného provozu, což je esenciální podmínkou zabezpečovacího systému pro ICT infrastrukturu provozující významné informační systémy dle zákona č. 181/2014, o kybernetické bezpečnosti.

## Požadavky na integraci

* Dodaný systém musí být integrovatelný na SIEM řešení IBM QRadar pomocí syslog protokolu a to tak, že musí umožnit zasílání zadavatelem vybraných bezpečnostních událostí systému minimálně v rozsahu definovaném v akceptačních testech.
* Dodaný systém musí být integrovatelný na provozní monitorovací nástroj zadavatele (Zabbix) tak, aby bylo možné monitorovat zadavatelem minimálně tyto běžné provozní metriky:
  + celkové zdraví zařízení
  + počet DNS dotazů v čase
  + počet zablokovaných dotazů v čase
  + množství živých agentů (poslední kontakt za X hodin)
* Dodaný systém musí disponovat rozhraním pro vyčítání dat (DNS logů) pro další analytické databázové nástroje (nepovinný požadavek, kvalitativní výhoda)
* Dodaný systém musí disponovat rozhraním pro vyčítání dat o instalovaných agentech (nepovinný požadavek, kvalitativní výhoda)
* Dodaný systém musí umožňovat definovat alerty, tedy typy událostí, které budou reportovány administrátorovi pomocí SMTP či syslog (nepovinný požadavek, kvalitativní výhoda)

## Ostatní požadavky

* Při analýze DNS provozu prostřednictvím Administračního portálu musí být možné vyhledávat a filtrovat pomocí minimálně těchto dvou metod:
  + textový zápis dotazů/filtrů pomocí klíčových slov a výrokové logiky (or, and, not)
  + výběr přednastavených možností filtrování (nepovinný požadavek, kvalitativní výhoda)
* Systém musí být dodaný a implementovaný tak, aby splnil veškeré akceptační testy definované v kapitole 1.5
* Všechny konfigurační změny a aktualizace musí být provedeny za plného provozu celého systému, přičemž tyto změny nesmí způsobit výpadky DNS služeb
* Možnost definování allow listů a deny listů pro vybrané IP segmenty
* Možnost definovat rozdílné bezpečnostní politiky pro různé IP segmenty (nepovinný požadavek, kvalitativní výhoda)

## Akceptační testy

Ověření funkcionality a požadované implementace bude ověřeno pomocí následujících akceptačních testů, které systém musí splnit. Testy budou probíhat ve společné součinnosti zadavatele a dodavatele. O splnění každého testu musí být poskytnut důkaz vhodnou formou (např. screenshot, textový záznam, apod.).

1. provedení DNS překladu požadavku zadavatelem vybrané domény ze zadavatelem vybraného klientského zařízení v interní síti LAN tak, že v logu systému budou jednoznačně rozpoznatelné minimálně tyto údaje:
   1. čas události překladu
   2. IP adresa zařízení
   3. typ dotazu (na jaký typ záznamu byl dotaz směřován)
   4. query
   5. response
2. provedení DNS překladu zadavatelem vybrané domény pomocí zadavatelem vybraného zařízení v páteřní síti tak, že v logu systému budou jednoznačně rozpoznatelné minimálně tyto údaje:
   1. čas události překladu
   2. veřejná IP adresa brány, která zprostředkovává připojení zařízení (IP adresa koncové sítě)
   3. typ dotazu (na jaký typ záznamu byl dotaz směřován)
   4. query
   5. response
3. provedení DNS překladu zadavatelem vybrané domény pomocí zadavatelem vybraného zařízení s OS MS Windows s nainstalovým klientem, umístěného ve veřejné síti Internet (resp. mimo lokální i páteřní síť) tak, že v logu systému budou jednoznačně rozpoznatelné minimálně tyto údaje:
   1. čas události překladu
   2. veřejná IP adresa brány, která zprostředkovává připojení zařízení
   3. typ dotazu (na jaký typ záznamu byl dotaz směřován)
   4. query
   5. response
4. provedení DNS překladu zadavatelem vybrané domény pomocí zadavatelem vybraného zařízení s OS Android s nainstalovanou klientskou službou umístěného ve veřejné síti Internet (resp. mimo lokální i páteřní síť) tak, že v logu systému budou jednoznačně rozpoznatelné minimálně tyto údaje:
   1. čas události překladu
   2. veřejná IP adresa brány, která zprostředkovává připojení zařízení
   3. typ dotazu (na jaký typ záznamu byl dotaz směřován)
   4. query
   5. response
5. provedení DNS překladu zadavatelem vybrané domény pomocí zadavatelem vybraného zařízení s OS IOS (Apple zařízení) s nainstalovanou klientskou službou umístěného ve veřejné síti Internet (resp. mimo lokální i páteřní síť) tak, že v logu systému budou jednoznačně rozpoznatelné minimálně tyto údaje:
   1. čas události překladu
   2. veřejná IP adresa brány, která zprostředkovává připojení zařízení
   3. typ dotazu (na jaký typ záznamu byl dotaz směřován)
   4. query
   5. response
6. provedení vyhledání libovolného DNS dotazu pomocí těchto filtrů, které mohou být zadavatelem libovolně kombinovány a skládány pomocí výrokové logiky (or, and, not):
   1. ip adresa zařízení (příp. brány)
   2. typ dotazu (na jaký typ záznamu byl dotaz směrován)
   3. typ hrozby
   4. libovolné časové okno
   5. dotazovaná doména
   6. DNS response
7. provedení automatického zablokování nebezpečného DNS dotazu ze zadavatelem vybraného zařízení tak, aby:
   1. tato blokace byla zřejmá v administračním portálu
   2. tato blokace přišla jako alert na zadavatelem vybranou e-mailovou adresu
   3. tato blokace byla založena jako alert a přenesena do stávajícího SIEM systému zadavatele přes syslog

Přičemž vybrané zařízení bude simulovat připojení k nebezpečné doméně. Nebezpečnost domény musí být v tomto případě vyhodnocena na základě threat intelligence a dalších automatických bezpečnostních mechanizmů systému.

1. provedení automatického zalogování nebezpečného DNS dotazu ze zadavatelem vybraného zařízení tak, aby:
   1. toto zalogování bylo zřejmé v administračním portálu
   2. toto zalogování bylo založeno jako alert a přenesena do stávajícího SIEM systému zadavatele přes syslog

Přičemž vybrané zařízení bude simulovat připojení k nebezpečné doméně. Nebezpečnost domény musí být v tomto případě vyhodnocena na základě threat intelligence a dalších automatických bezpečnostních mechanizmů systému.

1. zobrazení všech nebezpečných dotazů za posledních X dní, přičemž výsledek musí poskytnout informace o:
   1. zařízeních či IP adresách, které DNS dotazy prováděly
   2. typech a závažnostech hrozeb, které byli identifikovány

Přičemž zobrazená data je možné seskupit dle nejčastějších výskytů blokovaných domény případně zdrojových zařízení.

1. provedení automatického zablokování DNS dotazu ze zadavatelem vybraného zařízení tak, aby:
   1. tato blokace byla zřejmá v administračním portálu
   2. tato blokace byla přenesena do stávajícího SIEM systému zadavatele přes syslog

Přičemž vybrané zařízení bude simulovat připojení k doméně, která bude ručně uvedená na blacklistu pomocí politiky.

1. provedení automatického zablokování DNS dotazu ze zadavatelem vybraného zařízení tak, aby:
   1. tato blokace byla zřejmá v administračním portálu
   2. tato blokace byla přenesena do stávajícího SIEM systému zadavatele přes syslog

Přičemž vybrané zařízení bude simulovat připojení k doméně, která bude použita k simulovanému cílenému phishingovému útoku.

1. provedení automatického zablokování DNS dotazu ze zadavatelem vybraného zařízení tak, aby:
   1. tato blokace byla zřejmá v administračním portálu
   2. tato blokace byla přenesena do stávajícího SIEM systému zadavatele přes syslog

Přičemž vybrané zařízení bude simulovat připojení malware k doménám generovaným pomocí DGA.

## Požadavky na školení

Dodavatel provede školení a seznámení s používáním a obsluhou zadavatelem vybraných osob a to v rozsahu minimálně 1 MD.

## Požadavky na bezpečnost

Zadavatel požaduje, aby samotný systém (DNS resolvery a administrační portál) naplňoval tyto bezpečnostní požadavky v následujících oblastech:

### Kryptografie

Zadavatel stanovuje tyto podrobné požadavky na kryptografické funkce a algoritmy, tzn. že níže uvedené požadavky jsou pro dodavatele závazné, pakliže je jejich použití pro systém a jeho části relevantní.

#### Obecně

Pro šifrování, elektronické podepisování a provádění otisků dat (hashování) nesmí být použity proprietární/uzavřené algoritmy, ale ty, které jsou považovány za standardy, jejich funkcionalita je všeobecně známá

#### Hashovací funkce

##### Ukládání otisků hesel

* pro ukládání hesel uživatelů mohou být použity pouze tyto tzv. pomalé hashovací funkce:
  + Argon2 s parametry alespoň t=1, m=221, p=4 a funkcí Argon2id
  + scrypt s parametry alespoň N=32768 (215), r=8, a p=1
  + PBKDF2 s počtem iterací alespoň 100 000 a schválenou hašovací funkcí SHA-2 (viz níže)
* při hashování hesla musí být použit pseudonáhodně vygenerovaný kryptografický salt
* pro ukládání hesel nesmí být použity tzv. rychlé hashovací funkce typu MD-X, SHA-X, apod.

##### Elektronické podepisování e-mailů a dokumentů

* SHA-2 (SHA-256, SHA-384, SHA-512, SHA-512/256) a SHA-3 (SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256)
* délka otisku 384 bitů a vyšší

##### Ověřování integrity souborů

* SHA-2 (SHA-256, SHA-384, SHA-512, SHA-512/256) a SHA-3 (SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256)
* délka otisku 384 bitů a vyšší

#### Asymetrická kryptografie

##### SSL/TLS

* verze protokolu minimálně TLSv1.2 a vyšší
* konfigurace
  + cipher suite musí být vybrána na základě serverem preferovaného pořadí
  + vyšší priority musí mít cipher suites, které obsahují varianty asymetrických algoritmů s eliptickými křivkami, např.:
    - ECDHE musí mít vyšší prioritu než DHE
    - ECDSA musí mít vyšší prioritu než DSA
  + všechny EXPORT cipher suites musí být zakázány
  + algoritmy a funkce pro výměnu klíčů
    - algoritmus pro výměnu klíčů musí podporovat Perfect forward secrecy
      * tzn., že šifrovací klíč je vyměněn mezi klientem a serverem tak, aby jej nebylo možné získat se znalostí privátního klíče serveru, např. musí být použit Diffie-Hellman (DH nebo ECDH) algoritmus
      * a navíc se musí jednat o tzv. ephemeral Diffie-Hellman (DHE, ECDHE), tzn. že pro každou session je generován nový set Diffie-Hellman klíčů
    - délky klíčů:
      * pro Diffie-Hellman (DH) - 3072 bitů
      * pro Elliptic Curve Diffie-Hellman (ECDH) – 256 bitů a více
    - nesmí být použita anonymní výměna klíčů
  + algoritmy a funkce pro autentizaci
    - minimální délky klíčů:
      * RSA - 3072 bitů
      * DSA – 3072 bitů
      * ECDSA - 256 bitů
  + algoritmy a funkce pro symetrické šifrování
    - nesmí být použita hodnota NULL v cipher suites
    - nesmí být použity tyto šifry:
      * DES, 3DES, RC4
    - minimální délka šifrovacího klíče - 128 bitů
    - cipher suites s šiframi s větší délkou klíče musí mít větší prioritu v seznamu ciphersuites než s menší délkou klíče
  + MAC (Message Authentication Code)
    - použití SHA funkce s minimální délkou hashe 256 bitů
    - vyšší délky otisků musí mít vyšší prioritu v cipher suites

##### TLS cipher suites

* Doporučené cipher suites (v doporučeném pořadí), které naplňují výše zmíněné požadavky
* TLS1.3:

TLS\_AES\_256\_GCM\_SHA384

TLS\_CHACHA20\_POLY1305\_SHA256

TLS\_AES\_128\_GCM\_SHA256

TLS\_AES\_128\_CCM\_SHA256

* TLS1.2:

TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256

TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

TLS\_DHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256

#### Šifrování, podepisování a autentizace

* týká se různých technologií PKI, PGP, S/MIME, SSH, apod.
* minimální délka klíče
  + algoritmus DSA – 4096 bitů
  + algoritmus RSA - 4096 bitů
  + algoritmus ECDSA - 256 bitů
* Ověřování (např. SSH klíče)
  + délka klíče minimálně 4096 bitů u RSA a DSA algoritmů
  + délka klíče minimálně 256 bitů u algoritmů používajících eliptické křivky

#### Symetrická kryptografie

* nesmí být použity tyto šifry:
  + DES, 3DES, RC4, Blowfish, Kasumi
* minimální délka šifrovacího klíče - 128 bitů
  + pro šifru Chacha20 minimálně 256 bitů a se zatížením klíče menším než 256 GB
* nesmí být použity tyto módy pro ochranu integrity:
  + HMAC-SHA1, CBC-MAC-X9.19

### Logování a auditní záznamy

Zadavatel stanovuje základní požadavky na strukturu, formát, obsah, protokol a technickou konfiguraci auditních záznamů a logů zmíněných částí systému tak, aby měly tyto informace vypovídající hodnotu pro řešení a forenzní analýzu kybernetických bezpečnostních událostí.

#### Obsah auditních záznamů a logů

Auditní záznamy a logy zmíněných částí systému musí obsahovat minimálně tyto informace:

* přihlášení a odhlášení všech uživatelů (včetně administrátorů či jiných privilegovaných účtů),
* činnosti provedené administrátory, např. (pokud danou funkcionalitu obsahují):
  + přidělení/odebrání oprávnění,
  + založení/smazání uživatele
  + přidělení/odebrání role
  + reset hesla (pokud je prováděn na úrovni logujícího informačního aktiva)
  + povýšení oprávnění administrátora, převzetí role konkrétního uživatele
  + změna konfigurace logování událostí
  + změna konfigurace informačního aktiva,
* činnosti prováděné uživateli,
* automatická informační, varovná a chybová hlášení provozního charakteru (tzv. aplikační logy).

#### Struktura auditních záznamů a logů

Auditní záznamy a logy musí obsahovat minimálně tyto parametry a metadata:

* identifikátor události,
* identifikátor zdroje událostí,
* přesné datum vzniku události,
* přesný čas vzniku události včetně specifikace časového pásma,
* typ/název události,
* případně popis události (pokud není zřejmé z typu/názvu),
* jednoznačnou identifikaci účtu, pod kterým byla událost provedena,
* jednoznačnou síťovou identifikaci zařízení původce a
* úspěšnost nebo neúspěšnost (včetně neprovedení činnosti v důsledku nedostatečných oprávnění) události.

#### Úrovně auditních záznamů a logů

Zmíněné části systému musí zaznamenávat auditní záznamy a logy na všech existujících úrovních – tj. na úrovni:

* operačního systému aktiva v případě DNS resolverů,
* samostatné aplikace v případě administračního portálu

### Autentizace

Zadavatel stanovuje základní požadavky na bezpečnost přihlašování do administračního portálu. Autenizace na DNS resolverech bude probíhat standardními prostředky operačního systému.

Autentizace uživatelů do administračního portálu bude probíhat vůči externímu zdroji identit pomocí stávajícího SingleSignOn nástroje zadavatele (VysočinaID postavené na technologie SAML2).

### Autorizace

* Systém musí umožňovat granulární řízení přístupových oprávnění na základě aplikačních rolí.
* V případě autentizace vůči externímu zdroji identit musí být přidělování přístupových oprávnění (aplikačních rolí) založeno na uživatelských skupinách.
* Úrovně všech přístupových oprávnění/jednotlivých rolí musí být detailně popsány
  + např. formou popisu role v administračním rozhraní nebo v dokumentaci software
* Aplikační servery (např. DNS resolver daemon) nesmí vyžadovat pro své spuštění privilegovaná oprávnění (např. typu root, Administrator,apod.)

### Accounting

* Každý uživatel musí být unikátní (musí mít jednoznačný identifikátor) a personifikovaný.
* Nesmí existovat sdílený uživatel či sdílené heslo pro více uživatelů.
* Zrušení uživatele musí vždy probíhat formou jeho zneplatnění/zneaktivnění, nikoliv jeho vymazáním z důvodu zachování auditní stopy.

### Přenos dat

* Připojení k administračnímu portálu musí být vždy zabezpečené pomocí TLS protokolu a toto připojení musí být vynucováno.
* V případě on-premise instalovaného administračního portálu musí být možné nastavit komunikaci do sítě Internet přes aplikační HTTP proxy, která je systémově nastavená (případně lze konfigurovat přímo v portálu).
  + Dodavatel musí při implementaci on-premise administračního portálu vyspecifikovat všechny potřebné zdroje z internetu, které jsou nezbytné pro provoz systému za účelem vytvoření tzv. white-listu na aplikační HTTP proxy.

### HTTP Headers

Administrační portál musí naplňovat minimálně následující požadavky na bezpečnostní http hlavičky:

* X-Frame-Options
  + Musí být implementována (tzn. server ji musí klientské aplikaci zasílat) – v odůvodněných případech může být vynechána.
  + Záhlaví může nabývat pouze hodnot DENY nebo SAMEORIGIN dle potřeby
* Strict-Transport-Security
  + Musí být implementována
  + Direktiva max-age musí nabývat hodnoty minimálně 31536000
  + Ostatní direktivy jsou volitelné
* Content-Security-Policy
  + Musí být implementována
  + Aktiva mohou být načítána pouze prostřednictvím zabezpečeného protokolu (direktiva https:)
  + Aktiva mohou být načítána pouze z konkrétních a bezpečných zdrojů
  + Pokud by bylo nutné načítat aktiva z jiných zdrojů, které nejsou umístěny na infrastruktuře, která je v držení zadavatele a nebo dodavatele, podléhají tyto zdroje nejprve schválení zadavatelem.
* X-Content-Type-Options
  + Musí být implementována
* Referrer-Policy
  + Musí být implementována
  + Nesmí obsahovat direktivy: prázdný string, unsafe-url
* X-XSS-Protection
  + Musí být implementována
  + Directiva politiky musí nabývat hodnoty 1; mode=block
* Server
  + Pokud je hlavička implementována, musí být změněna tak, aby neodhalovala citlivé informace odhalující verzi webového serveru
* Set-Cookie
  + Pokud se jedná o session cookies, musí obsahovat direktivu nastavující secure a httponly flagy.
* Cross-Origin-Embedder-Policy
  + Musí být implementována

### Bezpečnostně provozní dokumentace

Zadavatel požaduje zpracování bezpečnostně provozní dokumentace k systému v rámci plnění zakázky v níže uvedeném rozsahu. Dodaná bezpečnostně provozní dokumentace může být i originální dokumentací výrobce, pokud pokrývá minimální požadavky uvedené v této zadávací dokumentaci. Akceptované jazyky provozní dokumentace jsou čeština a angličtina.

#### Bezpečnostní specifikace systému

Cíl dokumentu: popsat a zdokumentovat veškeré bezpečnostní mechanizmy a opatření za účelem identifikace toho, jaká data jsou jakým způsobem chráněna.

Forma dokumentu: textový popis

Minimální rozsah:

* Soupis a popis všech funkcí prosazujících bezpečnost pro:
  + zajištění integrity dat při jejich přenosu a uložení,
  + zajištění důvěrnosti dat při jejich přenosu a uložení,
  + zajištění autentizace a session managementu,
  + zajištění ošetření, filtrování a prověřování veškerých vstupních dat,
  + zajištění auditní stopy a logování,
  + externí rozhraní – jak uživatelská, tak pro komunikaci s externími systémy.
* Popis těchto oblastí:
  + použité kryptografické funkce a algoritmy,
  + autentizační a autorizační model a mechanizmus,
  + řízení uživatelských a privilegovaných rolí a oprávnění
  + detailní popis úrovně všech přístupových oprávnění/aplikačních rolí,
  + způsob zajištění dostupnosti, důvěrnosti a integrity dat ve stavech jejich uložení/uchování, zpracování a přenosu,
  + bezpečnostní architektura infrastruktury.

#### Instalace systému

Cíl dokumentu: popsat a zdokumentovat postupy, kroky a činnosti vedoucí k instalaci těch částí systému, které jsou instalované on-premise.

* Forma dokumentu: textová, může být doplněno o návodné obrázky.
* Systémové požadavky (architektura procesoru, verze operačního systému, minimální požadavky na HW, apod.)
* Instalační média a cesta k nim
* Konkrétní kroky vedoucí k instalaci systému

#### Základní konfigurace

Cíl dokumentu: popsat a zdokumentovat postupy, které vedou k nastavení systému do takového stavu, aby bylo možné systém po instalaci provozovat na základní úrovni.

Může se jednat např. o:

* Základní konfigurace sítě (nastavení ip adresa, maska, GW, ...)
* Nastavení připojení/komunikace na další systémy (např. DB, web server, SMTP, DNS, NTP, ...), nastavení portů na kterých služba naslouchá, kam data odesílá, …
* Nastavení proxy pro komunikaci, seznam URL (nebo domén), kam systém potřebuje komunikovat (směrem do Internetu), ...
* Spuštění potřebných modulů, agentů, komponent, procesů, registrování knihoven, úprava registrů OS Windows, …
* Nastavení automatických úloh, nastavení systémových účtů, …
* Detailní popis úrovně přístupových oprávnění/aplikačních rolí

#### Záloha, obnova, restart

Cíl dokumentu: popsat a zdokumentovat strategii zálohování systému, resp. návrh strategie zálohování od dodavatele, způsoby obnovy systému po havárii nebo ze zálohy, postupy a konkrétní kroky, které povedou k bezpečnému restartu systému.

* Zálohování
  + Strategie zálohování systému navržená dodavatelem
* Obnova
  + Posloupnost kroků (co a jak udělat), které je třeba provést pro obnovu systému nebo jeho části či dat ze zálohy do jeho plně funkčního stavu
  + Zpracovaný disaster recovery plán, tedy posloupnost kroků (co a jak udělat), které je třeba provést pro obnovu systému po jeho selhání do jeho plně funkčního stavu
    - Včetně potřebných zdrojů, jako je např. SW, HW, přístupové údaje, data, parametry disaster recovery prostředí, apod.
* Restart
  + Posloupnost kroků (co a jak udělat), které je třeba provést pro bezpečné restartování systému tak, aby naběhl do původního stavu
    - Např. informování uživatelů, ověření odhlášení všech uživatelů, provedení zálohy systému, restart systému (pořadí konkrétních procesů, služeb, apod.), způsob základní kontroly funkčnosti, výčet služeb, které je potřeba spustit/zkontrolovat, apod.

#### Monitoring

Cíl dokumentu: popsat a zdokumentovat mechanizmus monitorování a zaznamenávání bezpečnostních a provozních logů a auditních událostí.

* Popis logů informačního aktiva
* Popis možností provozního monitoringu (např. SNMP, síťový monitoring, aplikační monitoring) a návrh monitorovaných parametrů/metrik

#### Popis klíčových komponent

Cíl dokumentu: popsat a zdokumentovat účel, význam, úlohu a způsob použití klíčových komponent systému

* Forma dokumentu: textový popis/schéma)
* Základní účel jednotlivých klíčových komponent + jakou platformou (softwarem) jsou jednotlivé komponenty zajištěny