**Požadavek na změnu (RfC) Z27374**

**a – věcné zadání**

# Základní informace

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID SD MZe**[[1]](#endnote-2)**:** |  | **ID ShP MZe**[[2]](#endnote-3)**:** |  | **ID PK MZe**[[3]](#endnote-4)**:** |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Název změny**[[4]](#endnote-5)**:** | Upgrade serverů RedHAT na verzi 8.x – perimetr DMZ1 a DMZ2 | | | |
| **Datum předložení požadavku:** | | Klikněte sem a zadejte datum. | **Požadované datum nasazení:** | Klikněte sem a zadejte datum. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategorie změny**[[5]](#endnote-6)**:** | Normální  Urgentní | **Priorita**[[6]](#endnote-7)**:** | Vysoká  Střední  Nízká |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Oblas**t**:** | Aplikace | **Kód**[[7]](#endnote-8)**:** |  | Verze: | 6 |
| **Typ požadavku:** | Legislativní  Zlepšení  Reklamace  Bezpečnost | | |
| Infrastruktura | **Typ požadavku:** | Nová komponenta  Upgrade  Bezpečnost  Zlepšení  Obnova | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Jméno** | **Organizace /útvar** | **Telefon** | **E-mail** |
|  |  |  |  |  |
| Žadatel: | Pavel Štětina | **11152** | 2430 | Pavel.stetina@mze.cz |
| Metodický / věcný garant: | Pavel Štětina | **11152** | 2430 | Pavel.stetina@mze.cz |
| Change koordinátor: | Tomáš Kubíček | **11152** | 2473 | Tomas.kubicek@mze.cz |
| Poskytovatel / dodavatel: | xxx | **O2 CR a.s.** | xxx | xxx |

|  |  |  |  |
| --- | --- | --- | --- |
| **Smlouva č.**[[8]](#endnote-9)**:** | 470-2017-13330 | **KL:** | KL HR-001 |

# Stručný popis požadavku

## Popis požadavku

Na základě uveřejnění kritické zranitelnosti RedHAT – Kernel TCK SACK, bylo připraveno toto RFC pokrývající oblast upgrade serverů Perimetru DMZ1 a DMZ2 MZe. Vlastní RFC obsahuje i související aktivity nutné pro realizaci tohoto požadavku, jedná se především o následující:

* Příprava nového Kicstartu pro RedHAT 8.x
* Úprava a testy Ansible pro verzi RedHAT 8. (harrdening dle OKB, rozdělení site.yml na jednotlivé playbooky, ladění celé konfigurace na nový OS atd)
* Definice nových globálních pravidel pro nastavení lokálních FW v rámci DMZ1 MZe
* Definice a vyčištění hosts záznamů pro zónu DMZ1
* Součinnost provozovatele portálů eAGRI a EIP při změně rewrite proxy
* Součinnost provozovatele SAP při upgrade SAP routeru DMZ1
* Doplnění logování konfiguračních změn
* Jednotné nastavení serverů v DMZ1 pro penetrační scanování MZe a PIM MZe

## Odůvodnění požadované změny (legislativní změny, přínosy)

Odstranění kritické zranitelnosti TCP SACK na serveru v perimetru DMZ1 a DMZ2 MZe se souběžným upgrade na verzi RedHAT 8.x

## Rizika nerealizace

V případě nerealizace může dojít ke kompromitaci ICT Infrastruktury Mze.

# Podrobný popis požadavku / realizace

Na perimetru DMZ1 a DMZ2 je celkově 20 serverů, kterých se plánovaný upgrade týká. V seznamu nejsou uvedeny SSO, na kterých aktuálně probíhá upgrade na novou verzi SSO a OS dle schváleného RFC.

## Rozdělení serverů na perimetru:

* Proxy servery DMZ1 – reverzní proxy eAGRI, Externí portál
  + Celkem 8 ks serverů
  + Použité komponenty: hosts, lokální firewall, apache proxy, SSO agent, OMU agent
  + Nutná součinnost T-Softu při migraci, náklady jsou započítány do tohoto RFC
  + Migrace serverů bude realizováno za využití redundance prostředí, vždy bude odstaven jeden server ze dvojice, na kterém bude probíhat upgrade.

* Proxy servery DMZ2 – reverzní Interní portál, portál UKZUZ
  + Celkem 8 ks serverů
  + Použité komponenty: apache proxy, SSO agent, OMU agent
  + Nutná součinnost T-Softu při migraci, náklady jsou započítány do tohoto RFC
  + Migrace serverů bude realizováno za využití redundance prostředí, vždy bude odstaven jeden server ze dvojice, na kterém bude probíhat upgrade.
* Develop portál DMZ1 / DMZ2 – **tyto servery jsou vyjmuty z realizace tohoto RFC**
  + Celkem 2 ks serverů
  + Servery jsou vystavěny účelově pouze pro prostředí SharePoint 2013, náročnost přechodu na RedHAT 8.x je velmi vysoká, proto doporučujeme buď nasadit dočasné řešení vypnutí selektivního ACK nebo akcelerovat po dokončení RFC na SharePoint 2016 migraci na obsahu ze SharePointu 2013 a celé prostředí zrušit.
  + Servery nejsou předmětem tohoto RFC
* rproxy, saprouter DMZ1
  + Celkem 2 ks serverů
  + Použité komponenty: hosts, lokální firewall, DNS server, OMU agent, SAProuter – komunikační komponenta pro komunikaci se SAP Waldorf
  + Nutná součinnost SAP při zprovoznění komponenty na SAProuteru se souběžnou kontrolou kompatibility SAP Routeru verzus RHEL 8.x, pokud se ukáže že verz 8 ještě není ze strany SAP podporována, bude nainstalována verze 7.4 s opatchovaným jádrem.
  + Náklady SAP jsou započítány do tohoto RFC
  + Migrace serverů bude realizováno za využití redundance prostředí, vždy bude odstaven jeden server ze dvojice, na kterém bude probíhat upgrade. Komponenta SAP pro komunikaci do Waldorfu není redundantní, po dobu upgrade saprouteru nebude komunikace do SAP Waldorf dostupná.

**Důležité upozornění:**

* + Aktuální verze SSO agenta použitá v prostředí MZe nepodporuje verzi OS RedHAT 8.x, tedy reinstalaci Rewrite proxy eAGRI a E/I portálu bude možné zahájit až po dokončení a akceptaci RFC na upgrade SSO produkce a test – termín RFC je 11.11.2019. Před tímto datem bude probíhat příprava Kicstartu, ladění Ansible, ladění OS RedHAT 8.x a migrace serverů rproxy a SAP router.

## Seznam dotčených serverů

Žlutě označené servery nejsou vrámci tohoto RFC řešeny.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **IP** | **DMZ** | **Dev/Test/Prod** | **Description** | **OS version->Name** |
| n2rhpvd1 | 172.16.216.175 | DMZ1 | TEST | TEST - eAGRI rewrite node 1 | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpvd2 | 172.16.216.176 | DMZ1 | TEST | TEST - eAGRI rewrite node 2 | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpvd3 | 172.16.216.170 | DMZ1 | TEST | TEST - Externí portál rewrite node 1 | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpvd4 | 172.16.216.171 | DMZ1 | TEST | TEST - Externí portál rewrite node 2 | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpve1 | 172.16.216.145 | DMZ1 | PROD | PROD - eAGRI rewrite node 1 | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpve2 | 172.16.216.146 | DMZ1 | PROD | PROD - eAGRI rewrite node 2 | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpve3 | 172.16.216.140 | DMZ1 | PROD | PROD - Externí portál rewrite node 1 | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpve4 | 172.16.216.141 | DMZ1 | PROD | PROD - Externí portál rewrite node 2 | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpvy3 | 172.16.216.181 | DMZ1 | DEV | Develop Externí portál | Red Hat Enterprise Linux 6 (64-bit) |
| Rproxy | 172.16.216.12 | DMZ1 | PROD | rproxy | Red Hat Enterprise Linux 6 (64-bit) |
| Saprouter | 172.16.232.145 | DMZ1 | PROD | saprouter | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpvd5 | 172.17.101.129 | DMZ2 | TEST | TEST - Interní portál rewrite node 1 | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpvd6 | 172.17.101.130 | DMZ2 | TEST | TEST - Interní portál rewrite node 2 | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpve5 | 172.17.100.129 | DMZ2 | PROD | PROD - Interní portál rewrite node 1 | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpve6 | 172.17.100.130 | DMZ2 | PROD | PROD - Interní portál rewrite node 2 | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpvk3 | 172.17.105.133 | DMZ2 | TEST | TEST - Portal OSS UKZUZ | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpvk4 | 172.17.105.134 | DMZ2 | TEST | TEST - Portal OSS UKZUZ | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpvl3 | 172.17.104.133 | DMZ2 | PROD | PROD - Portal OSS UKZUZ | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpvl4 | 172.17.104.134 | DMZ2 | PROD | PROD - Portal OSS UKZUZ | Red Hat Enterprise Linux 6 (64-bit) |
| n2rhpvy2 | 172.17.166.149 | DMZ2 | DEV | Develop Interní portál | Red Hat Enterprise Linux 6 (64-bit) |

# Detailní popis činností

## KickStart MZe – RedHat Linux

V rámci realizace bude připraven nový image OS Rhel verze RHEL 8.x, kernel pro automatizovanou instalaci na nové fyzické a virtuální servery servery MZe.

* + Příprava nového KickStart image OS RHEL 8.x
  + Testy fungování nového image – zkušební instalace nových serverů na vybraný HW a do VM
  + Aktualizace dokumentace

## Rekonfigurace serveru pro správu konfigurací (Ansible)

V rámci přípravy prostředí Ansible budou provedeny následující kroky.

* Revize všech základních tasků a jejich atomizace na jednotlivé playbooky pro jednoduší odladění pod RHEL 8.x
  + zakládaní kont a skupin
  + nastavovaní prostředí pro OMU agenty, uživatele, systémové služby (ntp, postfix, ssh, syslog, stunnel, ...)
  + vypínaní nepotřebných služeb po defaultní instalaci
  + promazávaní některých logů
  + nastavovaní oprávnění k adresářům
  + instalace vybraných programů
  + atd.
* prvotní instalace OMU agenta
* hardeningu nového image bude realizováno dle change logu a Rhel 8 Hardening Policy OKB.
* Kontrola nastavení nově instalovaného serveru ze strany OKB
* Aktualizace dokumentace

Nastavení nové image bude provedeno dle Příloha číslo 1 – Change Log RedHat Linux (RHEL 7.2, kernel 3.10.0-327.28.3.el7) a Příloha číslo 2 – Rhel 7 Hardening Policy viz níže vložený soubor.



## Reinstalace jednotlivých VM a serverů

Postup je popsán v odstavci 3.1 Rozdělení serverů na perimetru.

## Logování konfiguračních změn

* Instalace auditd daemona na servery dle tabulky v odstavci 3.2
* Instalace bude provedena prostřednictvím Ansible – jak instalace auditd, tak nastavení logování
* Nastavení odesílání logů do SIEMu prostřednictvím syslogu na portu TCP/2515
  + 172.17.78.8
  + 172.17.78.9
* Konfigurace pluginu audisp pro logování auditních událostí na interní Syslog server
  + /etc/audisp/plugins.d/syslog.conf
    - active = yes
    - direction = out
    - path = builtin\_syslog
    - type = builtin
    - args = LOG\_INFO
    - format = string
  + Konfigurace pravidel auditd
    - /etc/audit/rules.d/audit.rules
    - # This file contains the auditctl rules that are loaded
    - # whenever the audit daemon is started via the initscripts.
    - # The rules are simply the parameters that would be passed
    - # to auditctl.
    - ## Smazani veskerych pravidel
    - -D
    - ## Nastaveni velikosti bufferu
    - -b 8192
    - ## Failure Mode 1 (printk) -f 1
    - ## Auditovani samotneho auditd - veskere pristupy a modifikace auditd logu
    - -w /var/log/audit/ -k auditlog
    - ## Auditovani samotneho auditd - veskere zmeny a upravy auditd konfigurace
    - -w /etc/audit/ -p wa -k auditconfig
    - -w /etc/libaudit.conf -p wa -k auditconfig
    - -w /etc/audisp/ -p wa -k audispconfig
    - ## Monitorovani pouzivani auditd nastroju
    - -w /sbin/auditctl -p x -k audittools
    - -w /sbin/auditd -p x -k audittools
    - ## Specialni soubory
    - -a exit,always -F arch=b32 -S mknod -S mknodat -k specialfiles
    - -a exit,always -F arch=b64 -S mknod -S mknodat -k specialfiles
    - ## Mount operace
    - -a exit,always -F arch=b32 -S mount -S umount -S umount2 -k mount
    - -a exit,always -F arch=b64 -S mount -S umount2 -k mount
    - ## Zmeny casu/data
    - -a exit,always -F arch=b32 -S adjtimex -S settimeofday -S stime -S clock\_settime -k time
    - -a exit,always -F arch=b64 -S adjtimex -S settimeofday -S clock\_settime -k time
    - ## Cron monitoring
    - -w /etc/cron.allow -p wa -k cron
    - -w /etc/cron.deny -p wa -k cron
    - -w /etc/cron.d/ -p wa -k cron
    - -w /etc/cron.daily/ -p wa -k cron
    - -w /etc/cron.hourly/ -p wa -k cron
    - -w /etc/cron.monthly/ -p wa -k cron
    - -w /etc/cron.weekly/ -p wa -k cron
    - -w /etc/crontab -p wa -k cron
    - -w /var/spool/cron/crontabs/ -k cron
    - ## Pristupy a zmeny dulezitych souboru ohledne uzivatelu, skupin a hesel
    - -w /etc/group -p wa -k etcgroup
    - -w /etc/passwd -p wa -k etcpasswd
    - -w /etc/gshadow -k etcgroup
    - -w /etc/shadow -k etcpasswd
    - -w /etc/security/opasswd -k opasswd
    - ## Zmeny hesel
    - -w /usr/bin/passwd -p x -k passwd\_modification
    - ## Monitorovani nastroju pro zmeny na uzivatelich a skupinách
    - -w /usr/sbin/groupadd -p x -k group\_modification
    - -w /usr/sbin/groupmod -p x -k group\_modification
    - -w /usr/sbin/useradd -p x -k user\_modification
    - -w /usr/sbin/usermod -p x -k user\_modification
    - -w /usr/sbin/adduser -p x -k user\_modification
    - ## Konfigurace site
    - -w /etc/hosts -p wa -k hosts
    - -w /etc/sysconfig/network-scripts/ -p wa -k network
    - ## Startovani systemu
    - -w /etc/inittab -p wa -k init
    - -w /etc/init.d/ -p wa -k init
    - -w /etc/init/ -p wa -k init
    - ## Zmeny localtime
    - -w /etc/localtime -p wa -k localtime
    - ## Parametry jadra
    - -w /etc/sysctl.conf -p wa -k sysctl
    - ## Konfigurace modprobe
    - -w /etc/modprobe.d/ -p wa -k modprobe
    - ## Konfigurace PAM
    - -w /etc/pam.d/ -p wa -k pam
    - -w /etc/security/limits.conf -p wa -k pam
    - -w /etc/security/pam\_env.conf -p wa -k pam
    - -w /etc/security/namespace.conf -p wa -k pam
    - -w /etc/security/namespace.init -p wa -k pam
    - ## Konfigurace SSH
    - -w /etc/ssh/sshd\_config -k sshd
    - ## Zmeny hostname
    - -a exit,always -F arch=b32 -S sethostname -k hostname
    - -a exit,always -F arch=b64 -S sethostname -k hostname
    - ## Zmeny issue
    - -w /etc/issue -p wa -k etcissue
    - -w /etc/issue.net -p wa -k etcissue
    - ## Vsechny zamitnute pristupy na kriticke prvky FS
    - -a exit,always -F arch=b64 -S open -F dir=/etc -F success=0 -k unauthedfileacess
    - -a exit,always -F arch=b64 -S open -F dir=/bin -F success=0 -k unauthedfileacess
    - -a exit,always -F arch=b64 -S open -F dir=/sbin -F success=0 -k unauthedfileacess
    - -a exit,always -F arch=b64 -S open -F dir=/usr/bin -F success=0 -k unauthedfileacess
    - -a exit,always -F arch=b64 -S open -F dir=/usr/sbin -F success=0 -k unauthedfileacess
    - -a exit,always -F arch=b64 -S open -F dir=/var -F success=0 -k unauthedfileacess
    - -a exit,always -F arch=b64 -S open -F dir=/home -F success=0 -k unauthedfileacess
    - -a exit,always -F arch=b64 -S open -F dir=/srv -F success=0 -k unauthedfileacess
    - ## Eskalace opravneni, zmena uzivatele, uprava sudoers
    - -w /bin/su -p x -k priv\_esc
    - -w /usr/bin/sudo -p x -k priv\_esc
    - -w /etc/sudoers -p rw -k priv\_esc
    - ## Vypinani a rebootovani serveru
    - -w /sbin/shutdown -p x -k power
    - -w /sbin/poweroff -p x -k power
    - -w /sbin/reboot -p x -k power
    - -w /sbin/halt -p x -k power
* Pokud jsou v uvedené konfiguraci pro auditd rozdíly v cestách k souborům na dané \*unixové distribuci, budou tyto rozdílné cesty v konfiguraci zohledněny k zajištění požadovaného auditování.

## Jednotné nastavení serverů v DMZ1 pro penetrační scanování MZe a PIM

Pro potřeby penetračního scanování MZe a PIM MZe bude upravena konfigurace FW serverů v DMZ1 a dále bude v DMZ1 povoleno pouze sshd přihlášení pomocí Private key.

**Nastavení prostupů na servery v DMZ1:**

* Protokol PING + SSH
* Vlan IP inf.
* 521 172.16.232.150 VULN
* 3521 172.16.216.20 VULN
* 3522 172.16.216.150 VULN
* 3523 172.16.216.169 VULN

**Nastavení prostupů pro PIM:**

Source IP Destination Port

172.17.191.217 TCP/22

172.17.191.218 TCP/22

172.17.191.219 TCP/22

172.17.191.209 TCP/22

172.17.191.210 TCP/22

172.17.191.201 TCP/22, ping

172.17.191.202 TCP/22, ping

10.19.21.49 TCP/22

10.19.21.50 TCP/22

10.19.21.41 TCP/22

10.19.21.42 TCP/22

Každý server v dané vlaně musí umožňovat přístup uvedenými protokoly z interface v příslušné vlaně, Na servery bude nahrán Public key PIMu, který zprostředkovává autentizaci pro VULN (potřebný Public key vygeneruje OKB MZe).

Toto nastavení všech serverů v DMZ1 bude pro všechny upgradované servery jednotné.

# Dopady na IS MZe

## Dopady

Změna verze OS dotčených serverů perimetru

## Požadavky na součinnost AgriBus

Není požadováno.

## Dotčené konfigurační položky

|  |  |  |
| --- | --- | --- |
| **ID** | **Název položky** | **Předpokládaný dopad** |
| 1 | n2rhpvd1 | Upgrade OS serveru |
| 2 | n2rhpvd2 | Upgrade OS serveru |
| 3 | n2rhpvd3 | Upgrade OS serveru |
| 4 | n2rhpvd4 | Upgrade OS serveru |
| 5 | n2rhpve1 | Upgrade OS serveru |
| 6 | n2rhpve2 | Upgrade OS serveru |
| 7 | n2rhpve3 | Upgrade OS serveru |
| 8 | n2rhpve4 | Upgrade OS serveru |
| 9 | Rproxy | Upgrade OS serveru |
| 10 | Saprouter | Upgrade OS serveru |
| 11 | n2rhpvd5 | Upgrade OS serveru |
| 12 | n2rhpvd6 | Upgrade OS serveru |
| 13 | n2rhpve5 | Upgrade OS serveru |
| 14 | n2rhpve6 | Upgrade OS serveru |
| 15 | n2rhpvk3 | Upgrade OS serveru |
| 16 | n2rhpvk4 | Upgrade OS serveru |
| 17 | n2rhpvl3 | Upgrade OS serveru |
| 18 | n2rhpvl4 | Upgrade OS serveru |

## Rizika implementace změny

V rámci toho RfC připadají následující rizika:

* Možné problémy se stabilitou serverů při použití nové verze RedHAT 8.x – především v oblasti apache verzus SSO agent

## Požadavek na podporu provozu naimplementované změny

(Uveďte, zda zařadit změnu do stávající provozní smlouvy, konkrétní požadavky na požadované služby, SLA.)

V rámci nasazení změny na produkční a testovací prostředí je požadována součinnost infra a zvýšený dohled i druhý den po nasazení.

## Požadavek na úpravu dohledového nástroje

(Uveďte, zda a jakým způsobem je požadována úprava dohledových nástrojů.)

Není požadování

# Požadavek na dokumentaci[[9]](#endnote-10)

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Název položky** | **Zpracovat**  (ANO/NE) | **Formát výstupu** (elektronické úložiště / CD / listinná forma) |
|  | Analýza navrhnutého řešení | NE |  |
|  | Dokumentace dle specifikace Závazná metodika návrhu a dokumentace architektury MZe[[10]](#endnote-11) | NE |  |
|  | Testovací scénář, protokol o otestování | NE |  |
|  | Uživatelská příručka | NE |  |
|  | Systémová příručka | ANO | Elektronické úložiště |
|  | Bezpečnostní dokumentace | NE |  |
|  | Profylaktické činnosti | NE |  |

# Akceptační kritéria

Plnění v rámci požadavku na změnu bude akceptováno, jestliže budou akceptovány dokumenty uvedené v tabulce výše v bodu 4 a provedeny činnosti dle bodu 3.2.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Akceptační kritérium** | **Způsob verifikace** | **Akceptuje** |
|  | Připravený kickstart + provedeny změny v Ansible | Kontrola deploymentu nového serveru | Pavel Štětina |
|  | Dotčené servery mají novou verzi OS, aplikace jsou funkční | Kontrola prostředí | Pavel Štětina |
|  | Dokumentace | Aktualizovaná dokumentace | Pavel Štětina |

# Podpisová doložka

|  |  |  |  |
| --- | --- | --- | --- |
| **Za resort MZe:** | **Jméno:** | **Datum:** | **Podpis:** |
| Metodický/Věcný garant | Pavel Štětina |  |  |
| Change koordinátor: | Tomáš Kubíček |  |  |

**B – nabídkA řešení k požadavku Z27374**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID ShP MZe**: |  | **ID PK MZe**: |  |

ID pro komunikaci s dod.: RFC\_INFRA\_2019\_NO022\_upgrade\_RHEL\_perimetr

# Návrh konceptu technického řešení

Viz část A tohoto RfC, body 2 a 3

# Uživatelské a licenční zajištění pro Objednatele

V souladu s podmínkami smlouvy 470-2017-13330.

# Dopady do systémů MZe

(Pozn.: V popisu dopadů zohledněte strukturu informací uvedenou v části A - Věcné zadání v bodu 4.U dopadů dle bodu 4.1 uveďte, zda může mít změna dopad do agendy, aplikace, na data, na síťovou strukturu, na serverovou infrastrukturu, na bezpečnost.)

# Dopady do agendy

Viz část A

# Dopady na aplikace

Viz část A

# Dopady na data

Viz část A

# Dopady na serverovou infrastrukturu

Viz část A

# Dopady na dohledové scénáře[[11]](#endnote-12)

Viz část A

# Dopady na bezpečnost

Návrh řešení musí být v souladu se všemi požadavky v aktuální verzi Směrnice systémové bezpečnosti MZe. Upřesnění požadavků směrnice ve vztahu k tomuto RfC:

|  |  |  |
| --- | --- | --- |
| **Č.** | **Oblast požadavku[[12]](#endnote-13)** | **Předpokládaný dopad a navrhované opatření/změny** |
|  | Řízení přístupu 3.1.1. – 3.1.6. | Viz část A |
|  | Dohledatelnost provedených změn v datech 3.1.7. | Viz část A |
|  | Centrální logování událostí v systému 3.1.7. | Viz část A |
|  | Šifrování 3.1.8., Certifikační autority a PKI 3.1.9. | Viz část A |
|  | Integrita – constraints, cizí klíče apod. 3.2. | Viz část A |
|  | Integrita – platnost dat 3.2. | Viz část A |
|  | Integrita - kontrola na vstupní data formulářů 3.2. | Viz část A |
|  | Ošetření výjimek běhu, chyby a hlášení 3.4.3. | Viz část A |
|  | Práce s pamětí 3.4.4. | Viz část A |
|  | Řízení - konfigurace změn 3.4.5. | Viz část A |
|  | Ochrana systému 3.4.7. | Viz část A |
|  | Testování systému 3.4.9. | Viz část A |
|  | Externí komunikace 3.4.11. | Viz část A |

# Dopady na síťovou infrastrukturu

(Pozn.: V případě, že má změna dopady na síťovou infrastrukturu, doplňte tabulku v připojeném souboru - otevřete dvojklikem.)



Viz část A

# Ostatní dopady

(Pozn.: Pokud má požadavek dopady do dalších požadavků MZe, uveďte je také v tomto bodu.)

Viz část A

# Požadavky na součinnost Objednatele a třetích stran

|  |  |
| --- | --- |
| **MZe / Třetí strana** | **Popis požadavku na součinnost** |
| ICT MZe | Umožnění plánovaných odstávek jednotlivých serverů pro potřeby migrace |
| ICT MZe | Součinnost při testování a ladění prostupů, aplikací a systémů |
| ICT MZe | Součinnost při kontrole OS RHEL 8.x |

(Pozn.: K popisu požadavku uveďte etapu, kdy bude součinnost vyžadována.)

# Harmonogram plnění[[13]](#endnote-14)

|  |  |
| --- | --- |
| **Popis etapy** | **Termín** |
| Realizace RFC dle zadání včetně dokumentace | T + 16 týdnů |
|  |  |

# Pracnost a cenová nabídka navrhovaného řešení

včetně vymezení počtu člověkodnů nebo jejich částí, které na provedení poptávaného plnění budou spotřebovány

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oblast / role**[[14]](#endnote-15) | **Popis** | **Pracnost v MD/MJ** | **v Kč bez DPH** | **v Kč s DPH** |
|  |  |  |  |  |
|  | Viz cenová nabídka v příloze č.01 | 71,88 | 471 643,75 | 570 688,94 |
| **Celkem:** | | 71,88 | 471 643,75 | 570 688,94 |

(Pozn.: MD – člověkoden, MJ – měrná jednotka, např. počet kusů)

# Přílohy

|  |  |  |
| --- | --- | --- |
| **ID** | **Název přílohy** | **Formát**  (CD, listinná forma) |
| 01 | Cenová nabídka, viz příloha č.1 | Listinná forma |
|  |  |  |

# Podpisová doložka

|  |  |  |  |
| --- | --- | --- | --- |
| **Název Dodavatele / Poskytovatele** | **Jméno** **oprávněné osoby**[[15]](#endnote-16) | **Datum** | **Podpis** |
| O2 Czech Republic, a.s. | xxx |  |  |

**C – Schválení realizace požadavku Z27374**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID ShP MZe**: |  | **ID PK MZe**: |  |

# Specifikace plnění

Požadované plnění je specifikováno v části A a B tohoto RfC.

Dle části B bod 3.2 jsou pro realizaci příslušných bezpečnostních opatření požadovány následující změny[[16]](#footnote-2):

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Oblast požadavku** | **Realizovat**  **(ano  / ne )** | **Upřesnění požadavku** |
|  | Řízení přístupu 3.1.1. – 3.1.6. |  |  |
|  | Dohledatelnost provedených změn v datech 3.1.7. |  |  |
|  | Centrální logování událostí v systému 3.1.7. |  |  |
|  | Šifrování 3.1.8., Certifikační autority a PKI 3.1.9. |  |  |
|  | Integrita – constraints, cizí klíče apod. 3.2. |  |  |
|  | Integrita – platnost dat 3.2. |  |  |
|  | Integrita - kontrola na vstupní data formulářů 3.2. |  |  |
|  | Ošetření výjimek běhu, chyby a hlášení 3.4.3. |  |  |
|  | Práce s pamětí 3.4.4. |  |  |
|  | Řízení - konfigurace změn 3.4.5. |  |  |
|  | Ochrana systému 3.4.7. |  |  |
|  | Testování systému 3.4.9. |  |  |
|  | Externí komunikace 3.4.11. |  |  |

# Uživatelské a licenční zajištění pro Objednatele (je-li relevantní):

# Požadavek na součinnost

|  |  |  |
| --- | --- | --- |
| **Útvar / Dodavatel** | **Popis požadavku na součinnost** | **Odpovědná osoba** |
|  |  |  |
|  |  |  |

# Harmonogram realizace[[17]](#endnote-17)

|  |  |
| --- | --- |
| **Popis etapy** | **Termín** |
|  |  |
|  |  |

# Pracnost a cenová nabídka navrhovaného řešení

včetně vymezení počtu člověkodnů nebo jejich částí, které na provedení poptávaného plnění budou spotřebovány

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oblast / role**[[18]](#endnote-18) | **Popis** | **Pracnost v MD/MJ** | **v Kč bez DPH:** | **v Kč s DPH:** |
|  |  |  |  |  |
|  | Viz cenová nabídka v příloze č.01 |  |  |  |
| **Celkem:** | |  |  |  |

(Pozn.: MD – člověkoden, MJ – měrná jednotka, např. počet kusů)

# Případné další obchodní podmínky[[19]](#endnote-19)

# Posouzení[[20]](#endnote-20)

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Jméno** | **Datum** | **Podpis/Mail[[21]](#endnote-21)** |
| Bezpečnostní garant | Roman Smetana |  |  |
| Provozní garant |  |  |  |
| Architekt |  |  |  |

# Schválení

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Jméno** | **Datum** | **Podpis** |
| Žadatel | Pavel Štětina |  |  |
| Věcný/metodický garant | Pavel Štětina |  |  |
| Change koordinátor | Tomáš Kubíček |  |  |
| Oprávněná osoba dle smlouvy | Pavel Štětina |  |  |

# Vysvětlivky

1. ID SD MZe – identifikátor požadavku přidělený v ServiceDesku MZe [↑](#endnote-ref-2)
2. ID ShP MZe – identifikátor projektu k požadavku přidělený v projektovém portálu MZe [↑](#endnote-ref-3)
3. ID PK MZe – identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe [↑](#endnote-ref-4)
4. Předmět změny – stručná informace, název požadavku [↑](#endnote-ref-5)
5. Kategorie změny – kategorie urgentní se využije v naléhavých případech, kdy je třeba vyřešit nedostupnost zásadní funkcionality systému vzhledem ke zpracování agendy, pro jejíž podporu systém slouží. [↑](#endnote-ref-6)
6. Priorita – vyjadřuje důležitost zapracování požadavku z pohledu časového. Vyplní se v případě volby kategorie „Normální změna“. [↑](#endnote-ref-7)
7. Kód – zkratka aplikace (viz „kód služby“ v katalogu služeb [↑](#endnote-ref-8)
8. Smlouva č. – uvede se, pokud existuje smlouva, v rámci níž se požadavky předkládají, totéž platí pro KL (katalogový list). [↑](#endnote-ref-9)
9. Vyplní Change koordinátor s Provozním garantem. [↑](#endnote-ref-10)
10. Rozsah požadované dokumentace uveďte pod tabulkou. [↑](#endnote-ref-11)
11. Pokud z vyhodnocení dopadů vyplyne potřeba upravit dohledové scénáře nebo zpracování nového scénáře, pak se má za to, že položka seznamu „Požadavek na dokumentaci“ v b. 5 části A RfC „Dohledové scénáře (úprava stávajících/nové scénáře)“ je vyžadována a bude součástí akceptačního řízení, nebude-li v části C RfC v bodu 1 „Specifikace plnění“ stanoveno jinak. [↑](#endnote-ref-12)
12. Jednotlivé oblasti – položky v tabulce korespondují s kapitolami Standardu systémové bezpečnosti. [↑](#endnote-ref-13)
13. Uvede se datum zahájení a ukončení realizace, příp. další etapy. [↑](#endnote-ref-14)
14. Role se vyplní pouze v relevantních případech, např. u požadavku na infrastrukturu. [↑](#endnote-ref-15)
15. Oprávněná osoba – smluvně určená osoba oprávněná k předkládání požadavku na předložení nabídky. [↑](#endnote-ref-16)
16. Potvrzení realizace příslušných opatření/změn vyznačí posuzovatel za Oddělení kybernetické bezpečnosti. [↑](#footnote-ref-2)
17. Uvede se datum zahájení a ukončení realizace, příp. další etapy. [↑](#endnote-ref-17)
18. Role se vyplní pouze v relevantních případech, např. u požadavku na infrastrukturu. [↑](#endnote-ref-18)
19. Změna smluvních podmínek - vyplní se v případě, že dohodnuté podmínky realizace požadavku se liší od smluvních. [↑](#endnote-ref-19)
20. RfC se zpravidla předkládá k posouzení Bezpečnostnímu garantovi, Provoznímu garantovi, Architektovi, a to podle předpokládaných dopadů změnového požadavku na bezpečnost, provoz, příp. architekturu. Change koordinátor rozhodne, od koho vyžádat posouzení dle konkrétního případu změnového požadavku. [↑](#endnote-ref-20)
21. Doplní se podpis nebo se uvede odkaz na mailovou zprávu, v které bylo posouzení doručeno. [↑](#endnote-ref-21)