Vzdálený přístup dodavatelů

Mgr. Tomáš Kovařík
Manažer kybernetické bezpečnosti - Nemocnice Jihlava p.o.

Požadavky normy a zákona

- Implementace ISMS dle ISO/EIC 27001:2014
  - Závazek vedení
  - Příloha A 9 Řízení přístupů
- Zákon č. 181/2014 Sb.
  - Provozovatel základní služby
  - §5 odstavec 2 - e) stanovení bezpečnostních požadavků pro dodavatele
- Vyhláška č. 82/2018 Sb.
  - §8 Řízení dodavatelů
  - §9 Bezpečnost lidských zdrojů

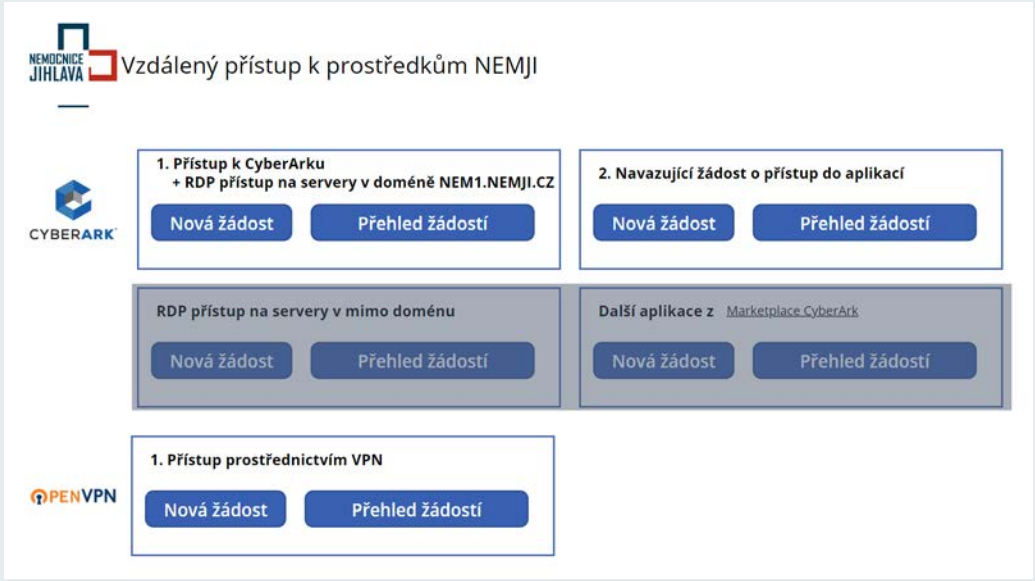
Ukotvení v NEMJI

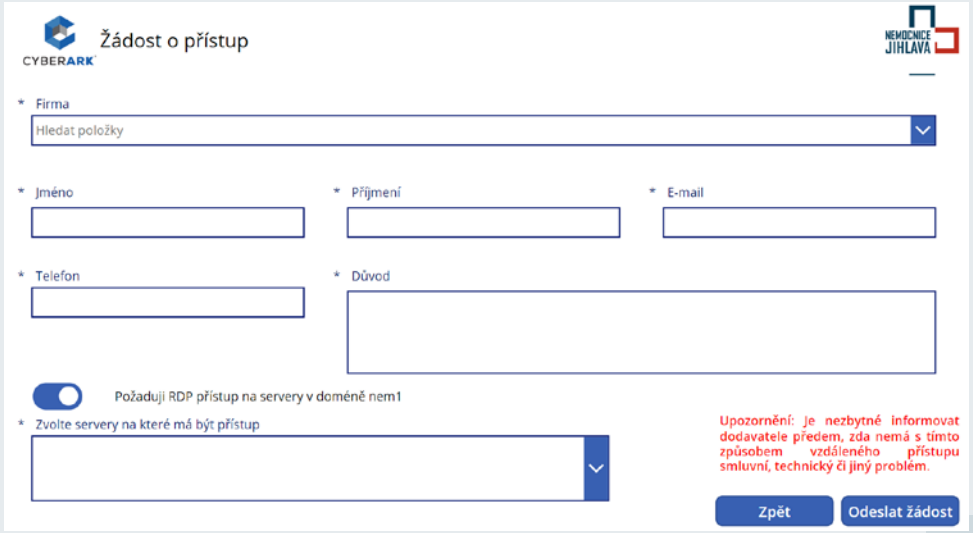
- Vyhlášení ISMS -> Bezpečnostní politika -> Politika řízení dodavatelů
- Bezpečnostní politika externí:
  - Pravidla pro přidělení
  - Technické řešení
  - Pravidla pro využívání
  - Přístup je řízen dle typu aktiva a jeho požadavků na kybernetickou bezpečnost.

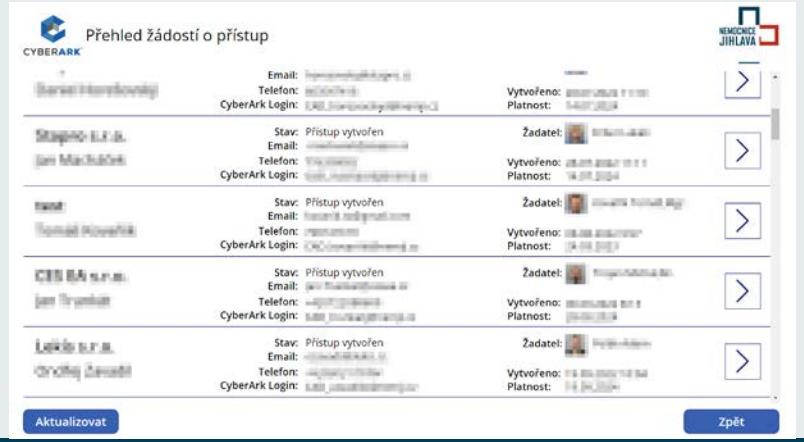
Procesní realizace v NEMJI

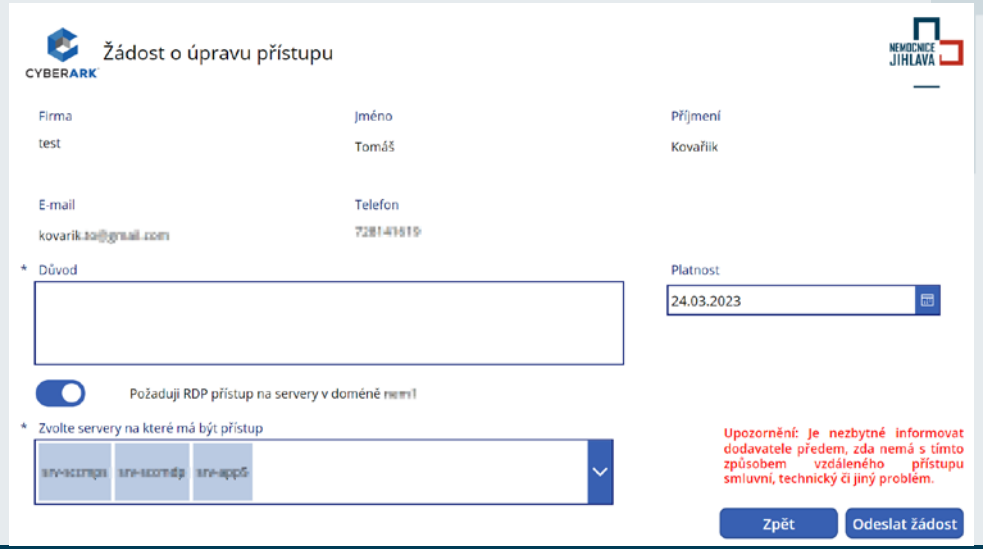
- M365 SharePoint Online
  - Evidence aktiv a serverů
  - Žádosti o vytvoření privilegovaného přístupu – schvalovací proces
  - Evidence privilegovaných přístupů
- Azure LogicApps integrované s evidencí
  - Žádosti při vzniku/zániku/prodloužení
  - Automatizace procesů
  - Notifikace
  - Integrace evidence s jednotlivými systémy
- PowerBI
  - Přehled napříč reálným stavem a evidencí – integrace dat zdrojů z evidence a reálných systémů

Aplikace žádostí o vzdálený přístup









Evidence žádostí

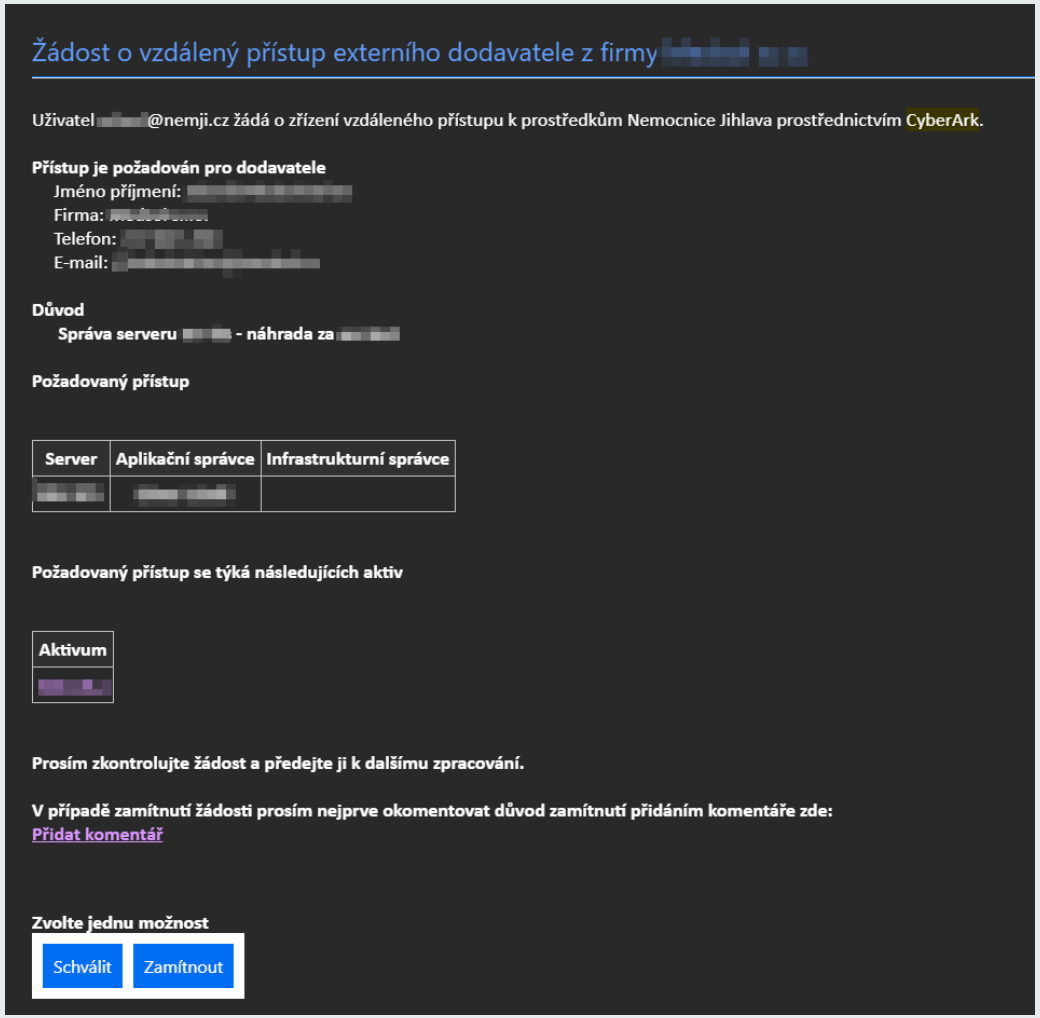
- Informace o aktuálním stavu

Žádost o přístup externího dodavatele - RDP ☆

Created	Žadatel	Stav	Schválení Mana...	Platnost	OTP	Poslední přihlášení	IP adresa ...	Město posledního při...	Firma
10/20/2022	[redacted]	Přístup vytvořen	✓ Ano	✓ 20. října	#microsoft.graph.pho	14. září	88.1[redacted]	Praha	[redacted]
31. ledna	[redacted]	Přístup vytvořen	✓ Ano	✓ 1/31/2024	#microsoft.graph.mic	úterý v 1:56 PM	80.1[redacted]	Praha	[redacted]
23. února	[redacted]	Přístup vytvořen	✓ Ano	✓ 2/23/2024	#microsoft.graph.mic	12. dubna	178.[redacted]5	[redacted]	[redacted]
7. června	[redacted]	Přístup vytvořen	✓ Ano	✓ 6/7/2024	#microsoft.graph.mic	12. září	80.1[redacted]	Praha	[redacted]
20. června	[redacted]	Přístup vytvořen	✓ Ano	✓ 6/20/2024	#microsoft.graph.mic	8. září	87.2[redacted]	Dolni[redacted]	[redacted]
20. června	[redacted]	Přístup vytvořen	✓ Ano	✓ 6/20/2024	#microsoft.graph.mic	před 2 hodinami	87.2[redacted]	Dolni[redacted]	[redacted]
12. července	[redacted]	Přístup vytvořen	✓ Ano	✓ 7/12/2024	#microsoft.graph.mic	19. července	80.1[redacted]	Praha	[redacted]
úterý v 11:29 AM	[redacted]	Proces selhal	✓ Ano	✓ 9/19/2024					[redacted]
Žadatel: Kovařík Tomáš,Mgr. (3)									
8/8/2022	Kovařík Tomáš,Mgr.	Přístup vytvořen	✓ Ano	⊗ 24. března	#microsoft.graph.mic	23. března	195.[redacted]2	Jihlava	test

Azure LogicApps

Schvalování žádosti o vzdálený přístup



Žádost o vzdálený přístup externího dodavatele z firmy [redacted]

Uživatel [redacted]@nemji.cz žádá o zřízení vzdáleného přístupu k prostředkům Nemocnice Jihlava prostřednictvím CyberArk.

Přístup je požadován pro dodavatele

Jméno příjmení: [redacted]
Firma: [redacted]
Telefon: [redacted]
E-mail: [redacted]

Důvod

Správa serveru [redacted] - náhrada za [redacted]

Požadovaný přístup

Server	Aplikační správce	Infrastrukturní správce
[redacted]	[redacted]	

Požadovaný přístup se týká následujících aktiv

Aktivum
[redacted]

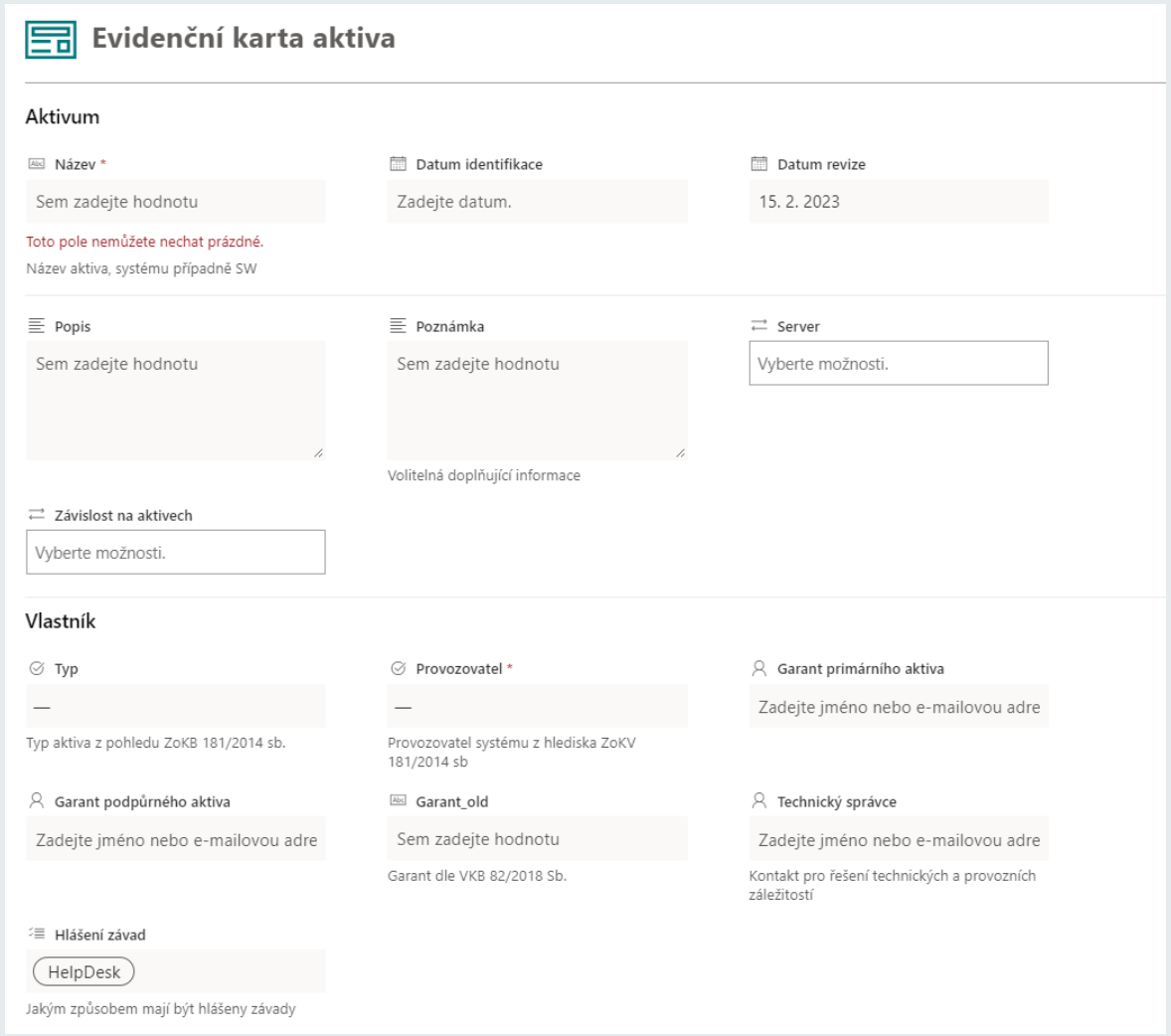
Prosím zkontrolujte žádost a předejte ji k dalšímu zpracování.

V případě zamítnutí žádosti prosím nejprve okomentovat důvod zamítnutí přidáním komentáře zde:
Přidat komentář

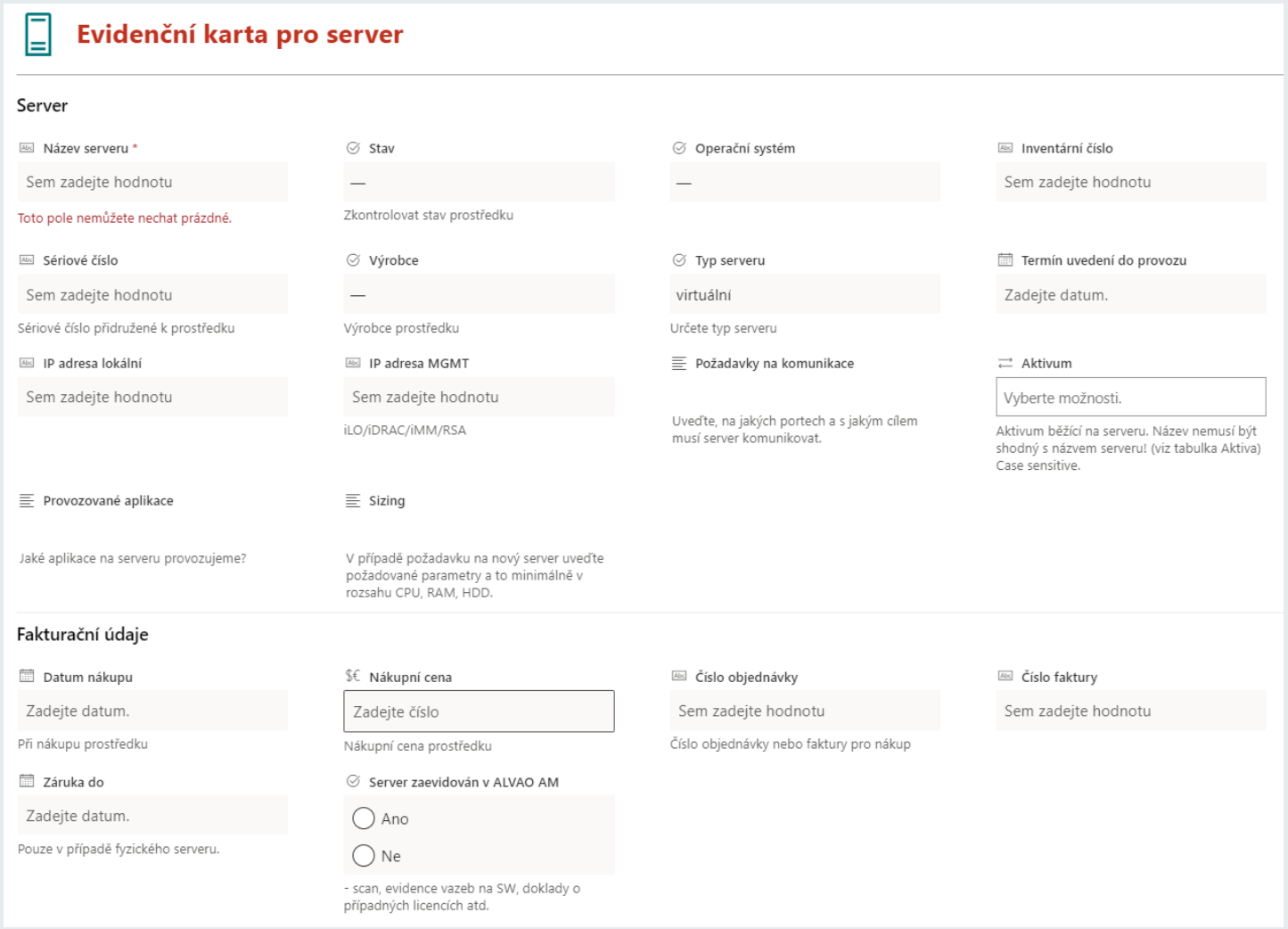
Zvolte jednu možnost

Schválit Zamítnout

Evidenční karta aktiva



Evidenční karta pro server



Evidenční karta pro server

Server

Název serveru *
Sem zadejte hodnotu
Toto pole nemůžete nechat prázdné.

Stav
—
Zkontrolovat stav prostředku

Operační systém
—

Inventární číslo
Sem zadejte hodnotu

Sériové číslo
Sem zadejte hodnotu
Sériové číslo přidružené k prostředku

Výrobce
—
Výrobce prostředku

Typ serveru
virtuální
Určete typ serveru

Termín uvedení do provozu
Zadejte datum.

IP adresa lokální
Sem zadejte hodnotu

IP adresa MGMT
Sem zadejte hodnotu
iLO/iDRAC/iMM/RSA

Požadavky na komunikace
Uveďte, na jakých portech a s jakým cílem musí server komunikovat.

Aktivum
Vyberte možnosti.
Aktivum běžící na serveru. Název nemusí být shodný s názvem serveru! (viz tabulka Aktiva) Case sensitive.

Provozované aplikace
Jaké aplikace na serveru provozujeme?

Sizing
V případě požadavku na nový server uveďte požadované parametry a to minimálně v rozsahu CPU, RAM, HDD.

Fakturační údaje

Datum nákupu
Zadejte datum.
Při nákupu prostředku

Nákupní cena
Zadejte číslo
Nákupní cena prostředku

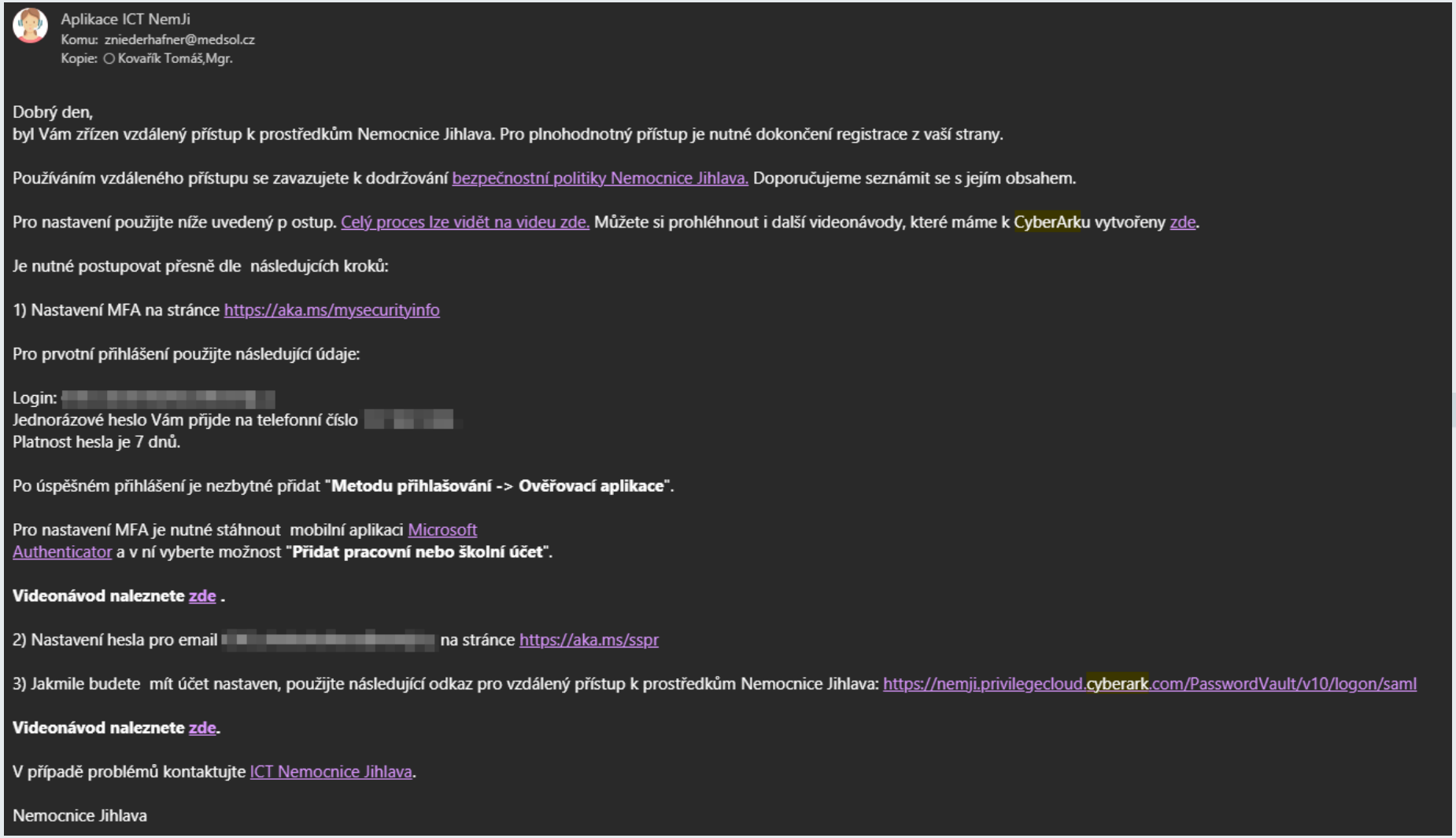
Číslo objednávky
Sem zadejte hodnotu
Číslo objednávky nebo faktury pro nákup

Číslo faktury
Sem zadejte hodnotu

Záruka do
Zadejte datum.
Pouze v případě fyzického serveru.

Server zaevidován v ALVAO AM
Ano
Ne
- scan, evidence vazeb na SW, doklady o případných licencích atd.

Uvítací email dodavateli



Aplikace ICT NemJi
Komu: zniederhafner@medsol.cz
Kopie: ○ Kovařík Tomáš,Mgr.

Dobrý den,
byl Vám zřízen vzdálený přístup k prostředkům Nemocnice Jihlava. Pro plnohodnotný přístup je nutné dokončení registrace z vaší strany.

Používáním vzdáleného přístupu se zavazujete k dodržování bezpečnostní politiky Nemocnice Jihlava. Doporučujeme seznámit se s jejím obsahem.

Pro nastavení použijte níže uvedený p ostup. Celý proces lze vidět na videu zde. Můžete si prohlédnout i další videonávody, které máme k CyberArku vytvořeny zde.

Je nutné postupovat přesně dle následujcích kroků:

1) Nastavení MFA na stránce https://aka.ms/mysecurityinfo

Pro prvotní přihlášení použijte následující údaje:

Login: [redacted]
Jednorázové heslo Vám přijde na telefonní číslo [redacted]
Platnost hesla je 7 dnů.

Po úspěšném přihlášení je nezbytné přidat "**Metodu přihlašování -> Ověřovací aplikace**".

Pro nastavení MFA je nutné stáhnout mobilní aplikaci Microsoft Authenticator a v ní vyberte možnost "**Přidat pracovní nebo školní účet**".

Videonávod naleznete zde .

2) Nastavení hesla pro email [redacted] na stránce https://aka.ms/sspr

3) Jakmile budete mít účet nastaven, použijte následující odkaz pro vzdálený přístup k prostředkům Nemocnice Jihlava: https://nemji.privilegecloud.cyberark.com/PasswordVault/v10/logon/saml

Videonávod naleznete zde.

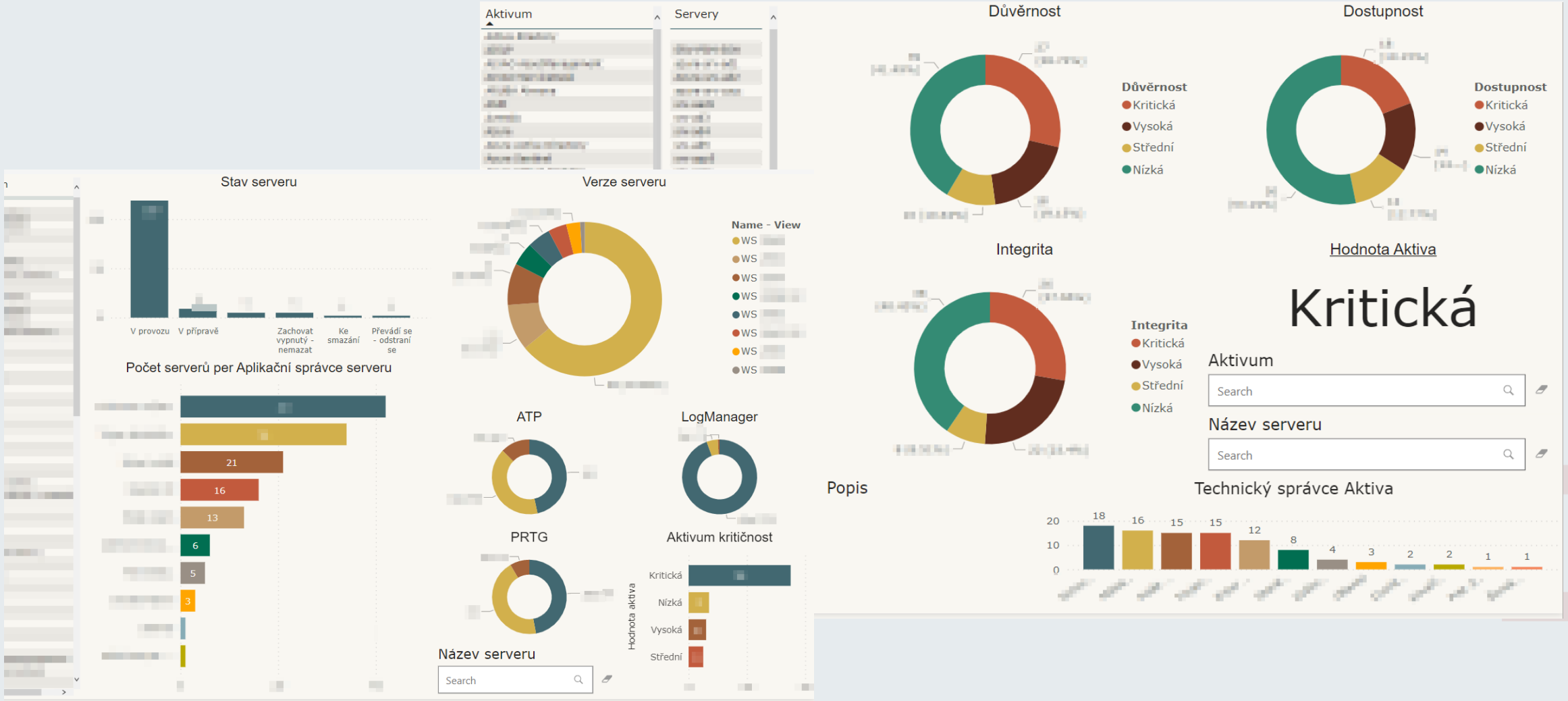
V případě problémů kontaktujte ICT Nemocnice Jihlava.

Nemocnice Jihlava

Video návod pro dodavatele

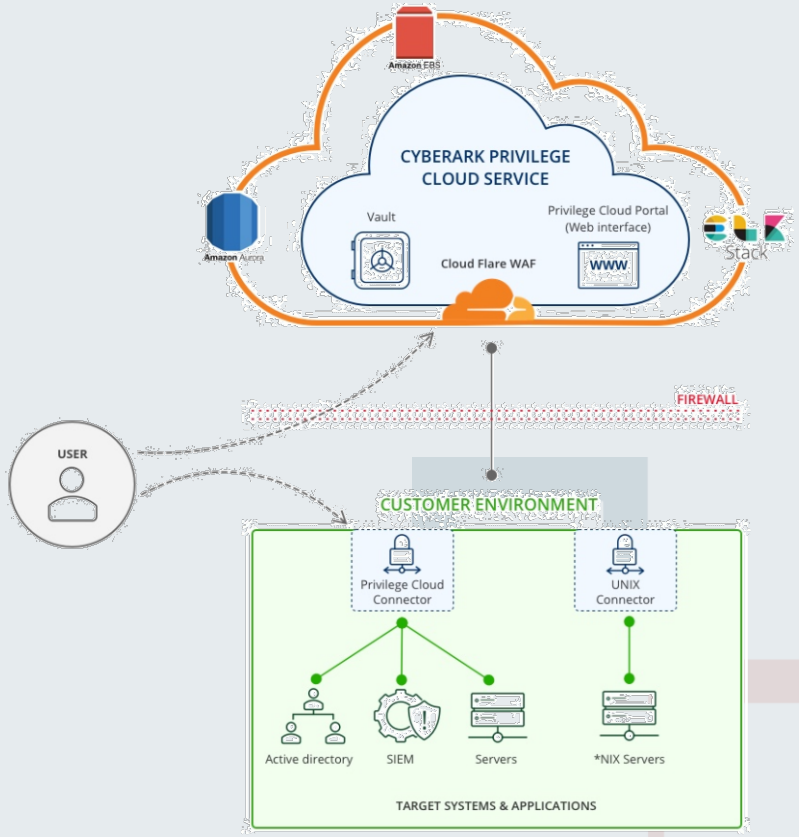
- Úvodní nastavení
- Používání privilegovaného přístupu

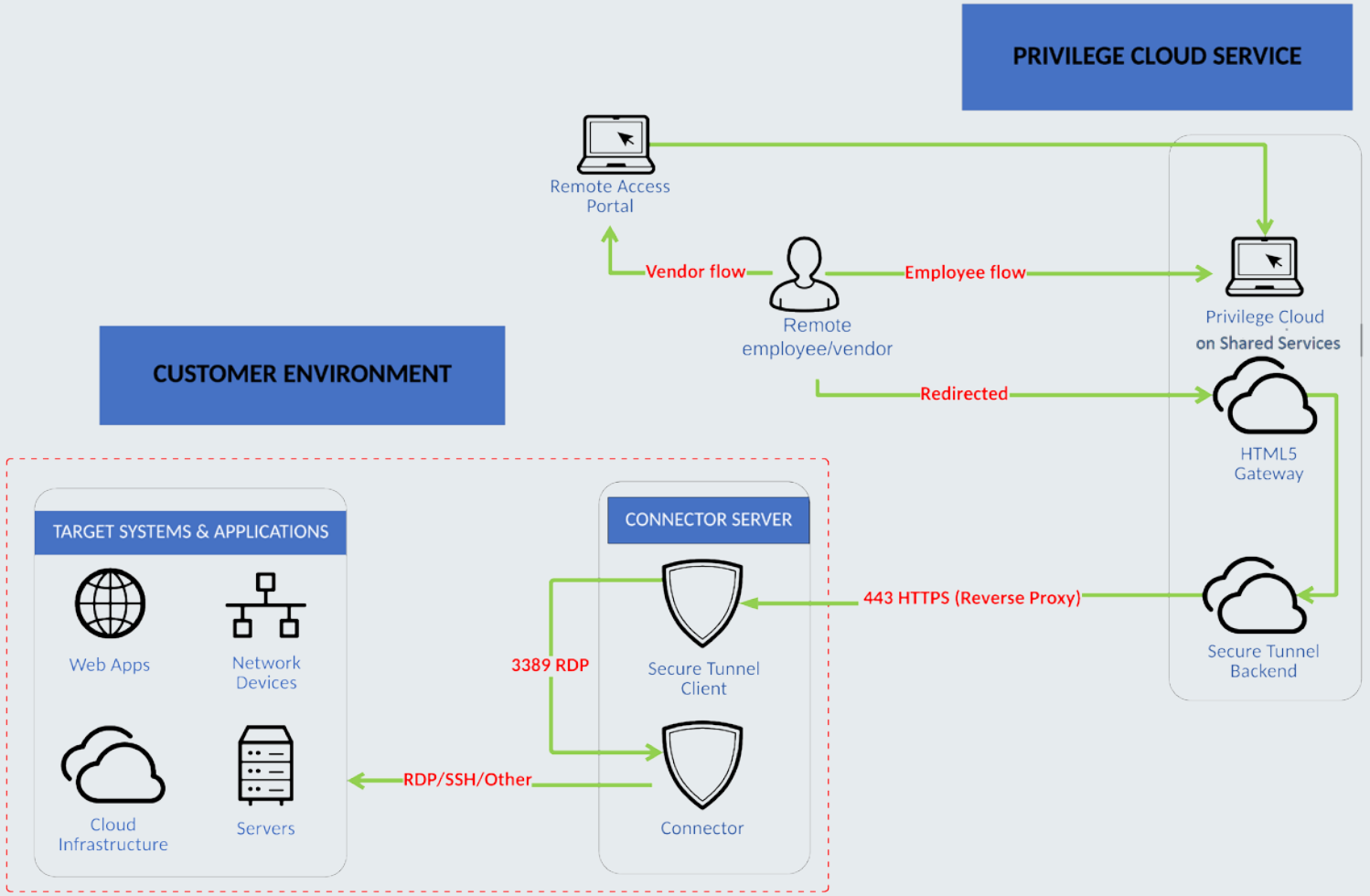
PowerBI


Aktivum
Servery
Stav serveru
V provozu
V přípravě
Zachovat vypnutý - nemazat
Ke smazání
Převádí se - odstraní se
Počet serverů per Aplikační správce serveru
21
16
13
6
5
3
Verze serveru
Name - View
WS
ATP
LogManager
PRTG
Aktivum kritičnost
Kritická
Nízká
Vysoká
Střední
Hodnota aktiva
Název serveru
Search
Důvěrnost
Dostupnost
Integrita
Hodnota Aktiva
Kritická
Aktivum
Search
Název serveru
Search
Popis
Technický správce Aktiva
20
10
0
18
16
15
15
12
8
4
3
2
2
1
1

Technická realizace v NEMJI

- CyberArk Privilege Cloud
  - SaaS řešení
  - PSM – systém řízení privilegovaných session
  - CPM – zajištění automatické rotace hesel
  - Není nutná žádná speciální aplikace pro přístup
  - MFA
  - Auditní stopa formou přepisu a videonahrávek
- Tradiční OpenVPN
  - Doplněk pro služby u kterých nelze použít
  - Auditní stopa na úrovni logů




PRIVILEGE CLOUD SERVICE
Remote Access Portal
Vendor flow
Employee flow
Remote employee/vendor
Privilege Cloud on Shared Services
CUSTOMER ENVIRONMENT
Redirected
HTML5 Gateway
TARGET SYSTEMS & APPLICATIONS
CONNECTOR SERVER
443 HTTPS (Reverse Proxy)
Web Apps
Network Devices
3389 RDP
Secure Tunnel Client
Secure Tunnel Backend
RDP/SSH/Other
Cloud Infrastructure
Servers
Connector

Děkuji za pozornost