Ministerstvo zdravotnictví České republiky
Palackého nám. č 4, 128 01 Praha 2, IČ: 00024341

Metodický pokyn poskytovatelům zdravotních služeb

k zajištění provozu ICT v mimořádné situaci

Pořadí revize	Provedené dne	Zpracoval	Schválil
Verze 1.01	20.3.2020	Tým autorů	Ing. Martin Zeman

Sledování dokumentu

Rozdělovník

JMÉNO	ORGANIZACE	PŘEDÁNO (dne)	Č. VÝTISKU
Archiv			

Historie verzí dokumentu

Verze	Vypracoval	Předmět	Datum
1.00	MZ ČR/ NCEZ	Ke zveřejnění	18.3.2020
1.01	MZ ČR/ NCEZ	Dílčí aktualizace na základě připomínek odborné veřejnosti	20.3.2020

Obsah

Seznam zkratek a pojmů

Zkratka	Význam
Active Directory	Implementace adresářových služeb LDAP od společnosti Microsoft
Best practice	Nejlepší praxe, osvědčené postupy v prací, díky nichž se dosáhlo dobrých výsledků v dané oblasti
Disaster recovery	Strategie pro zajištění obnovy IT služeb po živelních pohromách a katastrofách (včetně úspěšných kybernetických útoků a dalších stavů vedoucích ke zhroucení systému nebo omezení jeho provozu)
ICT	*Information and Communication Technologies* Informační a komunikační technologie
IS	Informační systém
LAN	*Local Area Net* Lokální (místní) počítačová síť
LDAP	*Lightweight Directory Access Protocol* Definovaný protokol pro ukládání a přístup k datům na adresářovém serveru
Matice RACI	Matice odpovědnosti RACI pro přiřazení a zobrazení odpovědnosti jednotlivých osob: • R - Responsible - kdo je odpovědný za vykonání úkolu • A - Accountable - kdo je odpovědný za celý úkol, je odpovědný za to, co je vykonáno • C - Consulted - kdo může poskytnout cenou radu či konzultaci k úkolu • I - Informed - kdo má být informován o průběhu úkolu či rozhodnutích v úkolu
NIS	Nemocniční informační systém
off-site záloha	Záloha nebo záložní kopie je kopie dat uložená na jiném datovém nosiči bez online propojení s informačním systémem, v ideálním případě uložená mimo běžný provozní perimetr (trezor, banka apod.)
PACS	*Picture Archiving and Communication System* Technologie ve zdravotnictví používaná pro zobrazování a zpracování obrazových dat. Představuje systém pro ukládání dat a přístup k nim.
RDP	*Remote Desktop Protocol* Síťový protokol, umožňující uživateli ovládat vzdálený počítač prostřednictvím počítačové sítě
SQL	*Structured Query Language* Strukturovaný dotazovací jazyk
SSH	*Secure Shell* Zabezpečený protokol, díky němuž dochází k připojení k serverům
TeamViewer	Aplikace pro přístup na vzdálenou plochu
VNC	*Virtual Network Computing* Vizuální program pro vzdálené připojení
VPN	*Virtual private network* Virtuální privátní síť

Tabulka 1 Seznam zkratek a pojmů

Význam každé zkratky uvedené v tabulce „Seznam zkratek a pojmů“ je nutné vykládat v souladu s platným právem ČR, EU a mezinárodními smlouvami, kterými je ČR vázána.

1 Vymezení účelu metodického pokynu

Metodický pokyn je určen pro poskytovatele zdravotních služeb a představuje výtah z příkladů nejlepší praxe (best practice), které popisují jednotlivé kroky pro zachování funkčních IT systémů nemocnice i v časech vyhlášení nouzového stavu.

Jednotlivé kroky vycházejí z podobných situací, z praxe již realizované některými velkými nemocnicemi a jsou souhrnem zkušeností a doporučení i ze zahraničí. Zároveň poskytuje vedení organizace, popř. jejímu zřizovateli, zakladateli či provozovateli, zpětnou vazbu k tomu, v jakém stavu se organizace nachází a kam se zaměřit pro zajištění provozu.

Dokument byl vypracován na základě iniciativy a s významným přispěním odborníků z Nemocnice Na Homolce a z Krajského úřadu Kraje Vysočina, jmenovitě pak Dušana Chvojky a Petra Pavlince a jejich spolupracovníků, kterým za tuto iniciativu patří náležité poděkování.

2 DOPORUČENÍ PRO ZAJIŠTĚNÍ PROVOZU A PODPORY ICT

2.1 IDENTIFIKACE KLÍČOVÝCH AKTIV

Identifikace klíčových informačních aktiv pro provoz organizace

Definujte důležité informační systémy (NIS, laboratorní IS, PACS, stravovací systém, e-mail apod.) a jejich podpůrné technologie (LAN, servery, virtualizační platforma, datová úložiště, identitní systémy (Active Directory, LDAP databáze), apod.) skutečně nezbytné pro řádný provoz organizace.

Identifikace klíčových personálních aktiv

Pro informační aktiva s největší prioritou zpracujte seznam rolí (např. RACI matice) jednotlivých osob s vazbou na tento systém, definujte klíčové kompetence a pracovníky pro zachování provozu informačního aktiva, případně pro jeho obnovu v rámci obnovy provozu v případě havárie nebo bezpečnostního incidentu.

Identifikace oslabených míst organizace

Identifikujte zařízení, na kterých uživatelé v běžné práci standardně využívají administrátorské účty pro běžnou práci, případně kde dochází ke sdílení jednoho účtu více uživateli (lékařské pokoje, vyšetřovny apod.)

2.2 DOKUMENTACE

Pro výše uvedená aktiva s nejvyšší prioritou zajistěte dokumentaci nezbytnou pro převzetí administrace a provozu jiným administrátorem, typicky v případě onemocnění nebo karantény části týmu. Součásti dokumentace by mělo být především:

- ✓ Administrátorská příručka
- ✓ Uživatelská příručka
- ✓ Popis architektury a klíčových komponent
- ✓ Systémové a administrátorské přístupy
- ✓ Technické poznámky: základní konfigurace, URL, IP adresy, postupy pro restart, umístění logů, mechanismy autentizace a autorizace, přenosové protokoly a porty, postupy řešení známých problémů, vazby na další systémy
- ✓ Kontakty na externí správce a dodavatele
- ✓ Popis mechanismu zálohování a obnovy

U klíčových a citlivých informací (např. přístupové údaje) doporučujeme jejich vytištění a uložení na bezpečné místo (např. zapečetěná obálka v trezoru). **Toto opatření je třeba provádět s ohledem na udržení důvěrnosti přístupových údajů!**

2.3 PERSONÁL – KLÍČOVÉ AKTIVUM ICT

Na základě zmapování klíčových informačních aktiv a rolí doporučujeme rozdělit tam, kde je to možné, jak administrátory (A), tak i techniky (B) do skupin:

A1. Klíčoví administrátoři: pracující striktně vzdáleně (homeoffice, režim karantény), do nemocnice mají vstup povolen jenom v krizové situaci.

A2. Operační administrátoři: pracující vzdáleně z domova, (homeoffice), v případě potřeby musí dorazit do cca max 3 hod na pracoviště v nemocnici.

B1. Operační skupina techniků ICT 1: tvoří první linii ICT podpory v nemocnici. Zůstávají na pracovišti, a to vždy ideálně dva na jednu směnu. Při výměně směn se navzájem technické týmy nesmějí fyzicky potkat.

B2. Operační skupina techniků ICT 2: pracující vzdáleně z domova (homeoffice) a řeší problémy z helpdesku. V případě potřeby musí dorazit do cca max 1 hod na pracoviště v nemocnici.

Tyto skupiny nesmí přicházet vzájemně do fyzického kontaktu, aby bylo maximálně zamezeno vzájemné kontaminaci a byla zajištěna jejich zastupitelnost v případě onemocnění.

Pro pracovníky přistupující vzdáleně je třeba zajistit odpovídající úroveň bezpečnosti používaných ICT prostředků a přenosových tras tak, aby nedocházelo ke kompromitaci nebo ohrožení systému v rámci vzdáleného přístupu. Homeoffice by tedy neměl být prováděn z domácích počítačů, ale výhradně ze zařízení pod úplnou bezpečnostní kontrolou organizace, připojení pak vždy po zabezpečené komunikační lince (VLAN, pevná IP adresa dedikovaná pro dané zařízení apod.).

2.4 EXTERNÍ PODPORA

Pokud je to organizačně a technicky možné, tak pro klíčové systémy doporučujeme zajištění záložní podpory (včetně zajištění případných procesů disaster recovery) pomocí externích kapacit dodavatelsky, typicky formou smlouvy o poskytování služeb na vyžádání.

2.5 PREVENCE KYBERNETICKÝCH ÚTOKŮ

S ohledem na stále se množící kybernetické útoky na zdravotnická zařízení, často zneužívající aktuální situace, doporučujeme věnovat výraznější pozornost kybernetické bezpečnosti. To znamená zejména dodržování následujících principů:

- ✓ Nastavení strategie zálohování (ideálně dle modelu 3-2-1) a její důsledná realizace
  - Stanovení typů záloh dle priority / dostupnosti
  - Kontrola funkčnosti / účinnosti / chybovosti záloh
  - Provádění záloh mimo provozní systémy a ukládání těchto záloh zcela mimo produkční prostředí informačního systému (off-site záloha)
  - Testování obnovy záloh, jejich konzistence (testování dostupnosti dat v zálohách, platnosti postupů obnovy, skutečné schopnosti obnovení systémů a dat)

- ✓ Zabezpečení perimetru LAN vůči veřejnému internetu – minimalizace otevřených portů a služeb (v žádném případě RDP, TeamViewer, VNC, SQL, SSH apod.)
- ✓ Urychlená aplikace záplat IS a OS (zejména serverových)
- ✓ Maximální segmentace sítě a minimalizace přístupu do internetu (využití blacklistů a whitelistů)
- ✓ Využívání vzdáleného přístupu přes VPN, jen pokud je to nutné
- ✓ Aplikace striktní politiky hesel (viz pravidla dle § 19 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti) a vynucení změny hesla u uživatelů, a to při nejmenším u těch, kteří mají možnost vzdáleného přístupu do organizace, zejména pak u dodavatelských účtů
- ✓ Striktní oddělení a separace používání uživatelských a administrátorských účtů
- ✓ Striktní zamezení využívání administrátorských účtů k běžným operacím na koncovém zařízení
- ✓ Striktní zákaz otevírat emaily a provádět emailovou komunikaci z účtů s administrátorskými oprávněními
- ✓ Optimalizace a pravidelná aktualizace antivirových a antispamových filtrů
- ✓ Monitoring a vyhodnocování síťového provozu – log na úrovni firewallu a proxy, NetFlow; je nutné vyhodnocovat alespoň 2x za pracovní dobu, a vždy do 30 minut po každé notifikaci události z alertovacích služeb nebo po oznámení NUKIB či jiného bezpečnostního zdroje
- ✓ Vedení aktuální evidence IP adresního plánu a evidence připojených zařízení do datové sítě (aktualizace vůči reálnému stavu nejméně jednou týdně), uložení evidencí tak, aby byly dostupné i v případě bezpečnostní události / incidentu
- ✓ Minimalizace offline cache hesel ve Windows
- ✓ Vzdělávání a informování uživatelů
    - Důsledné vzdělávání uživatelů v oblasti základních hygienických návyků práce s výpočetní technikou (práce s emailem, odkazy a přílohami, přístup na internet, práce s hesly, sociální sítě, cloudové služby, externí média apod.)
    - Upozornění uživatelů na množící se podvodné e-maily ohledně aktuálního tématu koronaviru – např. podvodné nabídky roušek a respirátorů, podvodné odkazy na nové informace ohledně šíření viru apod.
- ✓ Sledování informačních zdrojů:
    - V rámci Akčního výboru KB Ministerstva zdravotnictví (MS Teams, pro přihlášení do účasti v Akčním výboru a přístup do systému kontaktujte kb@mzcr.cz nebo přímo tomas.bezouska@mzcr.cz)
    - E-mailem (např. doporučení NÚKIB)
    - Aktuálně z bezpečnosti:
        - https://csirt.cz/cs/kyberbezpecnost/aktualne-z-bezpecnosti/
        - https://www.govcert.cz/cs/informacni-servis/hrozby/