

# Rámcová smlouva o zřízení a využívání vzdáleného přístupu

uzavřená dle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**“)

(dále jen „**Smlouva**“)

## Smluvní strany:

### 1. Fakultní nemocnice Bulovka

sídlo: Budínova 67/2, 180 81 Praha 8  
zastoupená: Mgr. Janem Kvačkem, ředitelem  
IČO: 00064211  
DIČ: CZ00064211  
bankovní spojení: Česká národní banka  
číslo účtu: 16231081/0710  
datová schránka: n9hiezm

(dále jen „**FNB**“)

**a**

### 2. Elanor a.s.

zapsaná: v obchodním rejstříku u Městského soudu v Praze, sp. zn.: B25583  
sídlo: Jemnická 1138/1, Michle, 140 00 Praha 4  
zastoupená: Mgr. Ajlou Bušinou, členkou představenstva  
IČ: 15887219  
DIČ: CZ15887219  
bankovní spojení: ČSOB, a.s.  
číslo účtu: 304931760/0300  
datová schránka: 8x53hba

(dále jen „**přístupovatel**“)

(FNB a přístupovatel společně jako „**smluvní strany**“ nebo jednotlivě jako „**smluvní strana**“)

## Úvodní ustanovení

- Přístupovatel prohlašuje, že zřízení a provoz vzdáleného přístupu, resp. přístupů, je pro něj nutným předpokladem pro řádné provádění podpory, údržby, aktualizací, upgradů či servisu v této Smlouvě uvedených systémů, aplikací či zdravotnických prostředků, které jsou v užívání FNB. Přístupovatel dále prohlašuje, že je schopen dodržet veškeré podmínky uvedené v této Smlouvě, zejména pak s ohledem na řádné využívání zřízeného vzdáleného přístupu smluvnými způsoby k provádění činností uvedených v předchozí větě.
- FNB prohlašuje, že je poskytovatelem zdravotních služeb, zejména dle zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování, ve znění pozdějších předpisů, jež za účelem naplňování svých povinností vyplývajících z právních předpisů, zřídila, provozuje a spravuje vlastní chráněnou datovou síť, do které přístupovatelé umožní omezený vzdálený přístup v rozsahu nezbytně nutném (dále jen „**vzdálený přístup**“) k výkonu provádění podpory, údržby, aktualizací, upgradů či servisu zařízení, systémů, přístrojů či aplikací spravovaných přístupovatelem (dále jen „**činnosti vzdálené správy**“), za podmínek vymezených touto Smlouvou.

## **Článek 1**

### **Předmět a účel Smlouvy**

1. FNB a přístupovatel touto Smlouvou sjednávají rámcové podmínky vzdáleného přístupu přístupovatele za účelem provádění činností vzdálené správy, která je nezbytným předpokladem pro řádné plnění Smlouvy o poskytování služeb komplexní podpory a rozvoje systému EGJE, HR portál, ESOI a jejich modulů uzavřené mezi smluvními stranami na základě výsledku zadávání veřejné zakázky s názvem „**Poskytování servisní podpory systému EGJE, HR portál a jejich modulů a další rozvoj**“ (výše uvedená smlouva pro účely této Smlouvy dále jako „**smlouva na veřejnou zakázku**“), která byla zadávaná FNB v otevřeném nadlimitním zadávacím řízení v souladu s ustanovením § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.
2. FNB se zavazuje, že umožní přístupovateli vzdálený přístup do chráněné datové sítě FNB (dále jen „**DS FNB**“) prostřednictvím VPN za účelem provádění činností vzdálené správy k produktům definovaným ve smlouvě na veřejnou zakázku, zejména pro provádění vzdálené správy, servisu a odstraňování poruch a/nebo vad produktů po dobu trvání smlouvy z veřejné zakázky, při současném splnění všech podmínek v této Smlouvě uvedených.
3. Technický postup zřízení vzdáleného přístupu do DS FNB, příp. jeho další eventuální technické varianty budou přístupovateli sděleny bez zbytečného odkladu po podpisu této Smlouvy. Na tyto technické postupy, příp. jejich event. varianty se vztahuje povinnost mlčenlivosti a FNB tímto výslovně prohlašuje, že tyto informace považuje za důvěrné a za informace neveřejného charakteru.
4. FNB se zavazuje zřídit vzdálený přístup do DS FNB bez zbytečného odkladu po doručení písemného požadavku přístupovatele, nebude-li mezi smluvními stranami písemně domluveno jinak.
5. Smluvní strany konstatují, že ke dni uzavření této Smlouvy došlo ke zřízení, tj. jsou již provozovány vzdálené přístupy do DS FNB pro činnosti vzdálené správy, servisu, upgrade, testování, implementace atp. jejichž bližší popis (včetně označení zařízení, systémů, přístrojů či aplikací a jejich aktuálního počtu) je uveden v Příloze č. 1 Smlouvy, která tvoří její nedílnou součást. Není-li v době podpisu této Smlouvy smluvními stranami zřízen a/nebo provozován žádný vzdálený přístup do DS FNB, je obsah Přílohy č. 1 Smlouvy prázdný.
6. Účelem Smlouvy je zakotvit způsob zřizování a definovat podmínky provozování vzdáleného přístupu do DS FNB do budoucna, jakož i stanovit pravidla a mantinely využívání zřízeného přístupu při činnostech vzdálené správy ze strany přístupovatele.

## **Článek 2**

### **Doba a místo plnění**

1. Zřízení a zajištění vzdáleného přístupu do DS FNB pro přístupovatele je ze strany FNB garantováno minimálně po dobu trvání smlouvy na veřejnou zakázku, nedojde-li k ukončení této Smlouvy dříve některým z dalších způsobů v ní uvedených.
2. Místem plnění je sídlo přístupovatele, popř. jiné místo, kde je umístěno zařízení, systém, přístroj či aplikace spravovaná přístupovatelem, a pro kterou je zřízen a využíván vzdálený přístup do DS FNB dle této Smlouvy a současně jsou přístupovatelem prováděny činnosti vzdálené správy.

## **Článek 3**

### **Práva a povinnosti smluvních stran**

1. Vzdálený přístup do DS FNB je poskytován výhradně přístupovateli nebo jeho zaměstnancům a zástupcům (viz Příloha č. 1 této Smlouvy), přičemž FNB tímto výslovně přístupovateli zakazuje jej dále převádět na jinou osobu či osoby.
2. V případě, že ze smlouvy na veřejnou zakázku uzavřené mezi FNB a přístupovatelem vyplývá oprávnění pro poddodavatele, resp. subdodavatele přístupovatele realizovat a tedy podílet se na plnění částí předmětu plnění ze smlouvy na veřejnou zakázku jménem přístupovatele, může FNB

umožnit vzdálený přístup do DS FNB těmto poddodavatelům/subdodavatelům, a to při splnění podmínky, že přístupovatel prokazatelně seznámí s obsahem a povinnosti vyplývajícími z této Smlouvy přísl. poddodavatele/subdodavatele. Okamžikem zřízení vzdáleného přístupu do DS FNB ze strany FNB pro poddodavatele/subdodavatele přístupovatele, odpovídá přístupovatel za řádné splnění povinností dle této Smlouvy ze strany jeho poddodavatelů/subdodavatelů tak, jako by tyto povinnosti plnil sám.

3. Veškeré technologie umístěné v FNB potřebné pro vzdálený přístup přístupovatele do DS FNB, nastavení a změny nastavení přístupu přístupovatele, internetová konektivita, licence, a služby spojené s údržbou vzdáleného přístupu do DS FNB zajišťuje FNB i přístupovatel v rámci součinnosti bezplatně.
4. Přístupovatel se zavazuje, že vzdálený přístup do DS FNB bude iniciovat pouze ze zařízení, které je dostatečně zabezpečené, tj.:
  - a) má instalován a pravidelně aktualizován program na ochranu proti škodlivému software,
  - b) má instalován pouze takový software, který byl instalován v souladu s licenčními podmínkami daného software, je
  - c) chráněno heslem,
  - d) má aktivní šifrování datového úložiště a pravidelně aktualizovaný operační systém, a
  - e) aktivovány funkce automatického uzamknutí v případě nečinnosti.

FNB je oprávněna splnění těchto požadavků kdykoli zkontrolovat, a to v sídle přístupovatele, či v jakémkoliv jiném místě, ze kterého je prováděn vzdálený přístup dle této Smlouvy. Přístupovatel je povinen FNB tuto kontrolu bezodkladně umožnit.

5. Přístupovatel se zavazuje, že vzdálený přístup do DS FNB bude využívat jen za účelem uvedeným v této Smlouvě, případně ve smlouvě na veřejné zakázce. Porušení této povinnosti je považováno za podstatné porušení Smlouvy, jež opravňuje FNB k okamžitému odstoupení od této Smlouvy. Přístupovatel je oprávněn v DS FNB nebo prostřednictvím DS FNB provádět pouze činnosti, které jsou potřebné k řádnému a bezchybnému provádění činností vzdálené správy, servisu, upgrade, testování, implementace atp. k zařízením, systémům, přístrojům či aplikacím, ke kterým dostal přístupovatel oprávnění od FNB, konkrétně navrženým manažerem kybernetické bezpečnosti FNB a schváleným náměstkem úseku informačních a komunikačních technologií FNB. Jiné činnosti má přístupovatel striktně zakázáno provádět.
6. Přístupovatel je povinen po/při každém vstupu do DS FNB sdělit odpovědí na e-mail s přihlašovací tokenem odeslaným z kontaktní adresy uvedené v odst. 11 tohoto článku, ve kterém popíše důvod ke vstupu do DS FNB, resp. sdělí, jaké činnosti včetně změn provedl/bude případně ještě provádět, prostřednictvím vzdáleného přístupu (postačí obecný popis, např. „Vstup do DSFNB úprava databáze“). Jakékoliv neoznámení tohoto vstupu přístupovatele ve lhůtě do 3 kalendářních dnů od jeho realizace, je považováno za porušení této Smlouvy. Bude-li se toto porušení povinností ze strany přístupovatele opakovat ve třech a více případech, zakládá to právo FNB od této Smlouvy okamžitě odstoupit.
7. Dále je přístupovatel povinen zajistit, že veškeré technické prostředky jím využívané pro vzdálený přístup do datové sítě FNB nebudou přístupné žádné neoprávněné osobě; zjistí-li přístupovatel ztrátu či kompromitování přihlašovacích údajů či certifikátů nebo má-li přístupovatel či jeho zaměstnanci nebo zástupci podezření na pokus o získání přihlašovacích údajů či certifikátů neoprávněnou osobou, nahlásí tuto skutečnost neprodleně na kontaktní adresu FNB uvedenou v odst. 12 tohoto článku Smlouvy.
8. Přístupovatel je povinen zajistit ochranu získaných neveřejných informací i jakýchkoliv dalších informací a dat získaných na základě vzdáleného přístupu dle této Smlouvy takovým způsobem, aby nemohlo dojít k jejich zneužití třetí osobou či samotnými zaměstnanci přístupovatele.

9. Přístupovatel se zavazuje učinit taková opatření, aby jeho zástupci či zaměstnanci zachovávali mlčenlivost o veškerých skutečnostech, osobních údajích a datech, o nichž se dozvěděli při plnění předmětu této Smlouvy, včetně těch, které eviduje pomocí prostředků a zařízení výpočetní techniky. Omezení ve vztahu k mlčenlivosti se nevztahuje na technické informace a data ve vztahu k zařízením uvedeným v článku 1 odst. 2 Smlouvy, které neobsahují údaje, které svým charakterem jsou nebo mohou být považovány za důvěrné či hodné ochrany dle příslušné právní úpravy a pokud se tyto informace vztahují k prováděné činnosti vzdálené správy zřízené a využívané dle této Smlouvy. Přístupovatel je tedy oprávněn nakládat pouze s informacemi, které jsou nezbytně potřebné k provádění činností uvedených v článku 1 odst. 2 Smlouvy. Za porušení tohoto závazku mlčenlivosti se považuje i využití těchto údajů a dat pro vlastní prospěch přístupovatele, prospěch třetí osoby nebo pro jiné účely. Přístupovatel bere na vědomí, že závazek mlčenlivosti není časově omezen.
10. Přístupovatel je povinen jednat dle pokynů FNB a veškerých vnitřních předpisů FNB týkající se chování a užívání DS FNB, se kterými FNB přístupovatele seznámila před podpisem této Smlouvy. Přístupovatel prohlašuje, že jsou mu tyto vnitřní předpisy FNB známy a bude se jimi řídit a zachovávat je.
11. Přístupovatel je povinen pravidelně se seznamovat s aktuálními pokyny a doporučeními Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“), přičemž se zavazuje tyto pokyny v co možná nejvyšší míře dodržovat. Bezpečnostní doporučení NÚKIB pro administrátory platná ke dni podpisu této Smlouvy tvoří její přílohu č. 1.
12. V případě oznamování přístupu do DS FNB dle odstavce 6 tohoto článku, jakýchkoliv změn nebo problematických otázek souvisejících s touto Smlouvou, či v případě důvodného podezření na možnost narušení bezpečnosti, je smluvní strana povinna o tom informovat druhou smluvní stranu, a to bez zbytečného odkladu na dále uvedené kontaktní údaje smluvních stran.
  - a) Kontaktní údaje FNB jsou následující: e-mail: █████@bulovka.cz, telefon: █████  
**v pracovní dny (aktivní v časech od 7.00 – 15.30 hod.), resp. █████ (aktivní v časech mezi 15:30 do 7:00 hod.).**
  - b) Kontaktní osobou přístupovatele je: e-mail: █████@elanor.cz, telefon: +420 █████ (od: 9:00 do: 16:00).
13. FNB je oprávněna kdykoli ukončit přístupovateli vzdálený přístup do DS FNB bez jakýchkoli sankcí vůči FNB, a to zejm. v případě možného ohrožení nebo okamžitého narušení bezpečnosti DS FNB. Sdělení důvodu ukončení vzdáleného přístupu do DS FNB však není podmínkou platnosti ukončení, FNB je oprávněna vzdálený přístup ukončit i bez uvedení důvodu. Odebrání přístupů z důvodů mimo stranu Přístupovatele nebo bez uvedení důvodu může být posuzováno jako neposkytnutí potřebné součinnosti pro plnění dle odst. 1 Úvodního ustanovení Smlouvy.
14. Porušení smluvních povinností přístupovatele stanovených v tomto článku zakládá právo FNB od Smlouvy kdykoli odstoupit.
15. Smluvní strana je oprávněna ukončit tuto Smlouvu kdykoliv písemnou výpovědí s výpovědní lhůtou dvou měsíců, která započne běžet prvním dnem kalendářního měsíce následujícího po měsíci, v němž byla výpověď doručena druhé smluvní straně.
16. Odstoupení FNB od této Smlouvy nemá vliv na povinnost přístupovatele uhradit smluvní pokutu dle této Smlouvy, nebo vliv na nárok FNB požadovat po přístupovateli náhradu škody.
17. Odstoupení nebo výpověď musí být učiněny pouze v písemné formě a musí být doručeny druhé smluvní straně osobně, doporučenou poštovní zásilkou nebo datovou schránkou.

#### **Článek 4** **Sankční ujednání**

1. V případě porušení povinností přístupovatele uvedených v článku 3 odst. 4, 5 a/nebo povinností přístupovatele uvedených v článku 9 Smlouvy, je přístupovatel povinen uhradit FNB smluvní pokutu ve výši 10 000 Kč (slovy: deset tisíc korun českých), a to za každý jednotlivý případ porušení některé z výše uvedených povinností.
2. V případě porušení povinností přístupovatele uvedené v článku 3 odst. 8 a/nebo 9 Smlouvy je přístupovatel povinen uhradit FNB smluvní pokutu ve výši 2 000 Kč (slovy: dva tisíce korun českých) za každý jednotlivý případ porušení této povinnosti.
3. Smluvní pokuty dle tohoto článku jsou splatné ve lhůtě 14 dnů ode dne, kdy oprávněná smluvní strana vyzve povinnou smluvní stranu k příslušné úhradě.
4. Uplatněním smluvní pokuty není dotčeno právo FNB na náhradu škody v plné výši, vzniklé FNB v důsledku porušení povinnosti utvrzené smluvní pokutou, a rovněž tím není dotčena povinnost přístupovatele splnit své povinnosti dle této Smlouvy.

#### **Článek 5** **Závěrečná ustanovení**

1. Tato Smlouva nabývá platnosti a účinnosti dnem jejího podpisu poslední smluvní stranou.
2. Smluvní strana je oprávněna ukončit tuto Smlouvu kdykoliv písemnou výpovědí z jakéhokoliv důvodu, nebo bez uvedení důvodu, s výpovědní lhůtou jednoho měsíce, která započne běžet prvním dnem kalendářního měsíce následujícího po měsíci, ve kterém byla výpověď doručena druhé smluvní straně.
3. V případě odstoupení od Smlouvy ze strany FNB účinky odstoupení nastávají dnem doručení tohoto písemného oznámení přístupovateli. Odstoupením od smlouvy není dotčena platnost kteréhokoliv ustanovení Smlouvy, jež má výslovně či ve svých důsledcích zůstat v platnosti i po skončení platnosti Smlouvy, zejména závazku mlčenlivosti a ochrany informací, zajištění a utvrzení závazků.
4. Tato Smlouva automaticky zaniká též dnem ukončení smlouvy na veřejnou zakázku, uvedeně v odstavci 1 článku 1 této Smlouvy. Smluvní strany jsou si následně povinny poskytnout veškerou nezbytnou součinnost k ukončení vzdáleného přístupu přístupovatele do DS FNB. Ustanovení věty druhé odst. 3 tohoto článku Smlouvy se použije přiměřeně.
5. Smluvní strany sjednávají, že měnit nebo doplňovat text Smlouvy je možné, s výjimkami ve Smlouvě výslovně uvedenými, pouze formou písemných dodatků podepsaných oběma smluvními stranami. Uzavření písemného smluvního dodatku není třeba pouze v případě změny údajů o smluvních stranách uvedených v záhlaví této Smlouvy, kontaktních osob nebo kontaktních údajů smluvních stran uvedených v článku 3 odst. 12 Smlouvy, kdy stačí písemné oznámení zaslané druhé smluvní straně. Smluvní strany se dále dohodly, že bude-li nezbytné aktualizovat obsah přílohy č. 1 Smlouvy, tato její aktualizovaná verze se stane platnou a účinnou ke dni, kdy obě smluvní strany vyjádří s jejím obsahem souhlas; pro tyto případy se nevyžaduje uzavření písemného smluvního dodatku ke Smlouvě.
6. Tato Smlouva a vztahy z této Smlouvy vyplývající se řídí právním řádem České republiky, zejména příslušnými ustanoveními občanského zákoníku.
7. Pokud některé z ustanovení této Smlouvy je nebo se stane neplatným, neúčinným či zdánlivým, neplatnost, neúčinnost či zdánlivost tohoto ustanovení nebude mít za následek neplatnost Smlouvy jako celku ani jiných ustanovení této Smlouvy, pokud je takovéto ustanovení oddělitelné od zbytku této Smlouvy. Smluvní strany se zavazují takovéto neplatné, neúčinné či zdánlivé ustanovení nahradit novým platným a účinným ustanovením, které svým obsahem bude co nejděleji odpovídat podstatě a smyslu původního ustanovení.

8. Smluvní strany se dohodly, že případné spory z této Smlouvy, nedojde-li k dohodě smluvních stran smírnou cestou, budou na návrh kterékoliv smluvní strany dány k rozhodnutí věcně a místně příslušnému soudu FNB.
9. Tato Smlouva je vyhotovena ve dvou stejnopisech s platností originálu. Každá ze smluvních stran obdrží po jednom stejnopisu této Smlouvy, jež má platnost originálu, nejedná-li se o případ, kdy je tato Smlouva vyhotovena v jediném elektronickém originálu, ke kterému zástupci smluvních stran připojí své elektronické podpisy.
10. Nedílnou součástí této Smlouvy jsou následující přílohy:
- Příloha č. 1 – Popis a informace o zřízených vzdálených přístupech
  - Příloha č. 2 – Bezpečnostní doporučení NÚKIB pro administrátory 4.0
11. Smluvní strany si před podpisem tuto Smlouvu řádně přečetly a svůj souhlas s obsahem jejich jednotlivých ustanovení stvrzují svým podpisem.

V Praze dne 10.4.2025

V Praze dne 3.4.2025

podepsáno elektronicky.....  
Mgr. Jan Kvaček  
ředitel  
**Fakultní nemocnice Bulovka**

podepsáno elektronicky.....  
Mgr. Ajla Bušina  
členka představenstva  
**Elanor a.s.**

Příloha č. 1 – Popis a informace o zřízených vzdálených přístupech

Přístupovatel aktuálně přistupuje na servery: 172.18.4.11, 172.18.2.16 a 172.18.2.103.  
Zaměstnanci přístupovatele, kteří mají udělen přístup:

@elanor.cz  
@elanor.cz  
@elanor.cz  
@elanor.sk  
@elanor.cz

# BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRÁTORY 4.0



## INFRASTRUKTURA



### **ČLEŇTE SÍŤ NA MENŠÍ CELKY (SEGMENTACE) A STRIKTNĚ ODDĚLUJTE UŽIVATELSKÁ PRÁVA NAPŘÍČ UŽIVATELI (SEGREGACE)**

s cílem oddělit citlivé informace a kritické služby typu autentizace uživatelů (např. Microsoft Active Directory) a vytvořit zóny s různou úrovní bezpečnostních omezení.

### **BLOKUJTE ŠKODLIVÉ IP ADRESY A DOMÉNYNA ÚROVNI GATEWAY (BLACKLISTY). NESAĎTE**

#### **SÍŤOVÉ SYSTÉMY DETEKCE / PREVENCE PRŮNIKU (IDS/IPS)**

používající signatury a heuristiky k identifikaci anomálního provozu v rámci sítě i překračujícího perimetr.

#### **SLEDUJTE SÍŤOVÝ PROVOZ**

pomocí vybraných síťových prvků nebo rozmístěním dedikovaných síťových sond. Sledujte komunikaci mezi klienty a servery, komunikaci klientů do internetu, komunikaci mezi servery i provoz na perimetru sítě a identifikujte provozní a bezpečnostní problémy.

#### **UCHOVÁVEJTE SÍŤOVÝ PROVOZ**

z/do kritických pracovních stanic a serverů a provoz překračující perimetr sítě pro případné forenzní zkoumání po průniku do sítě a systémů. Záznamy síťového provozu doporučujeme uchovávat po dobu minimálně 12 měsíců, více podle místních okolností a významu sítě – v případě kritické informační infrastruktury (KII) a u informačních systémů základní služby (PZS) podle zákona o kybernetické bezpečnosti a návazných vyhlášek je minimální lhůta 18 měsíců. V případě sítě strategického významu zvažte i možnost automaticky aktivovaného plného záznamu datového provozu (PCAP), a to jak na primárních, tak záložních systémech (např. webových nebo systémových serverech).

#### **KONTROLUJTE PŘÍCHOZÍ E-MAILY**

pomocí mechanismů Sender ID, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) a DMARC (Domain-based Message Authentication, Reporting and Conformance) a blokujte podvržené zprávy. Tyto mechanismy nastavte i pro možnou kontrolu odchozích zpráv druhou stranou.

#### **POUŽÍVEJTE ŠIFROVANÉ SPOJENÍ MEZI POŠTOVNÍMI SERVERY (TLS)**

pro zajištění důvěrnosti e-mailové komunikace, v ideálních případech použijte DANE (DNS- based Authentication of Named Entities). Kontrolu obsahu provádějte až poté, co je e- mailový provoz dešifrován.

#### **PROVÁDĚJTE AUTOMATIZOVANOU DYNAMICKOU ANALÝZU OBSAHU E-MAILŮ A WEBŮ**

prováděnou v sandboxu – hledejte podezřelé chování podle síťového provozu, tvorby nových souborů, úpravy stávajících souborů nebo změn konfigurace.

#### **POVOLTE NA FIREWALLU POUZE ŽÁDOUCÍ SLUŽBY A STANDARDNÍ PROVOZ.**

V případě koncových stanic nezapomeňte také blokovat spojení z Vámi nekontrolované sítě.

#### **KONTROLUJTE POUŽÍVANÉ KLÍČE / CERTIFIKÁTY**

především pro SSH autentizaci, webové servery, vzdálenou plochu apod. Kde je to možné, použijte šifrovanou komunikaci.

**ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ**  
(povolených a blokováných) s okamžitým automatickým vyhodnocováním a uložením po dobu minimálně 18 měsíců, více podle místních okolností a významu sítě.

**APLIKUJTE WHITELISTING WEBOVÝCH DOMÉN**

pro všechny domény – pokud to dovoluje charakter práce uživatelů. Tento přístup je účinnější než blacklistovat malé procento škodlivých domén.

**VOLTE JEDNODUCHÉ DOMÉNOVÉ NÁZVY,**

aby byly jasně viditelné případné záměny písmen ve phishingových e-mailech.

**NASAĎTE ANTI-DDoS TECHNOLOGIE,**

které můžete po důkladné úvodní analýze řešit buď vlastními silami, nebo ve spolupráci s poskytovatelem internetového připojení. Anti DDoS ochranu nasadte na kompletní IP rozsah vaší organizace.

**VYPRACUJTE DISASTER RECOVERY PLAN (DRP)**

a mějte připravené správné a funkční emailové adresy a telefonní čísla na ostatní administrátory, nadřízené pracovníky a CERT/CSIRT týmy.



————— **STANICE A SERVERY** —————



**UDRŽUJTE AKTUÁLNÍ OPERAČNÍ SYSTÉM**

pravidelnými aktualizacemi a v co nejkratší době aplikujte všechny vydané bezpečnostní záplaty.

**UDRŽUJTE AKTUÁLNÍ SOFTWARE,**

pravidelně kontrolujte verze instalovaného softwaru. U neaktuálního softwaru proveďte v rámci možností update. Zastaralé mohou být i verze použitých doplňků či modulů nebo firmware zařízení.

**NEPOUŽÍVEJTE NEPODPOROVANÉ PRODUKTY,**

používejte pouze produkty (software i operační systémy), pro které jsou dostupné bezpečnostní záplaty.

**OVĚŘUJTE IDENTITU APLIKACÍ A SOUBORŮ**

a povolte jen ty důvěryhodné včetně skriptů a DLL knihoven. V prostředí Windows použijte Device Guard, AppLocker, popřípadě Zásady omezení softwaru (SRP).

**PROVÁDĚJTE HARDENING KONFIGURACE UŽIVATELSKÝCH APLIKACÍ**

– povolte jen funkcionalitu, která je vyžadována pro práci uživatelů. Dodatečné funkce (např. Java a Flash ve webovém prohlížeči, makra v MS Office) povolte pouze, je-li to nutné.

**POUŽÍVEJTE OBECNÉ PREVENTIVNÍ MECHANISMY,**

které mohou pomoci ochránit systém před zero-day zranitelnostmi, jako např. DEP (Data Execution Prevention) nebo SELinux v linuxových systémech.

**AKTIVUJTE IDS/IPS SYSTÉMY NA KONCOVÝCH STANICÍCH**

detekující anomální chování jako např. injekci kódu do jiných procesů, změnu chráněných registrových klíčů, zachytávání stisků kláves, načítání neznámých ovladačů, snahu o zajištění perzistence a další.

### **ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ**

(povolených a blokováných) s okamžitým automatickým vyhodnocováním a uložením pro kritickou informační infrastrukturu (KII) a provozovatele základní služby (PZS) po dobu minimálně 18 měsíců, pro významné informační systémy (VIS) po dobu minimálně 12 měsíců a pro ostatní systémy podle místních okolností a významu sítě.

### **FILTRUJTE OBSAH E-MAILŮ A PROPOUŠTĚJTE POUZE RELEVANTNÍ DRUHY PŘÍLOH**

– po důkladné analýze chování uživatelů určete typy souborů, které potřebují posílat e- mailem. Ostatní formáty příloh blokujte – především spustitelný kód. Dále ověřujte soulad přípony souboru a jeho skutečného formátu.

### **PRAVIDELNĚ ZÁLOHUJTE DŮLEŽITÁ A CITLIVÁ DATA**

jako např. obsah webového serveru, databázi nebo konfiguraci služeb. Zálohu umístěte do odděleného prostředí mimo produkční síť. Pravidelně testujte, jestli dokážete data obnovit a jestli jsou data po obnově funkční.

### **ZAVEĎTE STANDARD OPERATING ENVIRONMENT (SOE)**

se standardizovanou konfigurací pro pracovní stanice i servery, kde budou vypnuty všechny nevyžádané funkcionality.

### **ZAMEZTE PŘÍMÉMU PŘÍSTUPU PRACOVNÍCH STANIC NA INTERNET**

a směrujte provoz přes split DNS server, e-mailový server nebo autentizovaný web proxy server. Nezapomeňte vynutit pro IPv4 i IPv6.

### **POUŽÍVEJTE ANTIVIROVÝ A BEZPEČNOSTNÍ SOFTWARE**

a nástroje, které zakazují spuštění nebezpečných aplikací (mimo přesně definovaný seznam privilegovaných aplikací), či nástroje, které pomáhají chránit systém v době, kdy nejsou dostupné klasické bezpečnostní aktualizace.

### **ŠIFRUJTE DISKY**

– zejména u přenosných počítačů – včetně centrální evidence klíčů.

### **VYUŽÍVEJTE TRUSTED PLATFORM MODULE (TPM),**

tedy zabezpečený kryptografický modul pro generování a uložení hesel a kryptografických klíčů, je-li jím počítač vybaven.

### **NASTAVTE HESLO UEFI / BIOS**

unikátní pro každou stanici s centrální správou hesel.

### **VYNUCUJTE SECURE BOOT**

a nastavte pořadí zařízení určených pro boot systému. Boot manager musí být zabezpečen heslem.

### **CHRAŇTE SE PŘED ÚTOKY NA HESLA**

u všech služeb, kam se přihlašují uživatelé. Například pomocí fail2ban, využití funkcí určených pro ukládání hesel (Argon2, bcrypt, scrypt, PBKDF2) nebo CAPTCHA.

### **PRO SPRÁVU SERVERŮ POMOCÍ SSH VYUŽÍVEJTE PRO PŘIHLÁŠENÍ KLÍČE, ZAKAŽTE HESLA**

Pro svázání otisku klíče se serverem, kde je použitý, využívejte SSHFP záznamy v DNS ideálně v kombinaci s DNSSEC, který zajistí autenticitu odpovědi obsahující SSHFP záznam.

### **PROVÁDĚJTE HARDENING KONFIGURACE SERVEROVÝCH APLIKACÍ**

tj. databází, webových aplikací, CRM systémů, účetních systémů, HR systémů a dalších systémů ukládání dat.

### **KONTROLUJTE PŘENOSNÁ MÉDIA**

jako součást širší strategie prevence ztráty dat, včetně vedení seznamu povolených USB zařízení, jejich skladování, šifrování, mazání a likvidace.

### **OMEZTE PŘÍSTUP K SERVER MESSAGE BLOCKU (SMB) A NETBIOSU**

na pracovních stanicích a serverech, kdekoliv je to možné.

### **POUŽÍVEJTE REŽIM CHRÁNĚNÉHO PŘÍSTUPU PŘI PRÁCI SE SOUBORY NA ÚROVNI PRACOVNÍCH STANIC**

může se např. jednat o Protected View nebo Protected mode.

### **VYNUŤTE VYTÁČENÍ VPN,**

pokud se zařízení připojuje mimo síť organizace. Omezte síťovou aktivitu, dokud není navázáno VPN spojení.

### **ZAJISTĚTE FYZICKOU BEZPEČNOST IT TECHNIKY**



## **SPRÁVA ÚČTŮ**



### **ZAVEĎTE CENTRÁLNÍ SPRÁVU UŽIVATELSKÝCH ÚČTŮ A OPRÁVNĚNÍ**

a nastavte jednotnou bezpečnostní politiku. Účtům, u kterých to není vyžadováno, odeberte rozšířená oprávnění a zakažte spouštění skriptů, instalaci softwaru, úpravy registru atd.

### **VYNUCUJTE VÍCEFAKTOROVOU AUTENTIZACI**

zejména pro akce vyžadující vyšší úroveň oprávnění a kritické operace jako vzdálený přístup nebo přístup k citlivým informacím.

### **ODDĚLTE ADMINISTRÁTORSKÉ ÚČTY**

Pro správu používejte speciální účty pro administraci systémů. Pro své ostatní pracovní aktivity (e-mail, web atd.) používejte běžný neprivilegovaný účet. Účet s oprávněním doménového administrátora je použit pouze ke správě Domain Controlleru (tzn. nepřistupuje na klientské stanice a servery).

### **PŘIDĚLTE KAŽDÉMU ADMINISTRÁTOROVÍ VLASTNÍ ÚČET**

pro správu systémů. Nepoužívejte sdílené účty.

### **ZABEZPEČTE LOKÁLNÍ ADMINISTRÁTORSKÉ ÚČTY.**

Nastavte unikátní heslo na každé stanici, v prostředí Windows můžete využít například LAPS (Local Administrator Password Solution).

### **VYNUŤTE POUŽÍVÁNÍ SILNÝCH HESEL**

s ohledem na vyžadovanou složitost, délku a dobu platnosti. Zamezte opakovanému použití stejných hesel a používání slovníkových výrazů. Vynuťte změnu hesla, existuje-li podezření, že bylo kompromitováno.

### **PRAVIDELNĚ KONTROLUJTE UŽIVATELSKÉ ÚČTY A JEJICH OPRÁVNĚNÍ**

a to jak lokální, tak centrálně spravované.

