

Rámcová smlouva o zřízení a využívání vzdáleného přístupu

uzavřená dle ust. § 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

se sídlem: Budínova 67/2, 180 81 Praha 8 - Libeň
zastoupená: Mgr. et Mgr. Jan Alexa, náměstek pro informační a komunikační technologie,
na základě pověření
IČO: 00064211
DIČ: CZ00064211
bankovní spojení: Česká národní banka
číslo účtu: 16231081/0710
datová schránka: n9hiez
(dále jen „**FNB**“)

a

2. Sefima s.r.o.

zapsaná: v obchodním rejstříku u Krajský soud v Ústí nad Labemsp. zn.: C 14943
sídlo: Lesní 461/41, Liberec XIV-Ruprechtice, 460 14 Liberec
zastoupená: RNDr. Václavem Vohánkou
IČO: 25048821
DIČ: CZ25048821
bankovní spojení: ČSOB, a.s.
č. účtu: 5885653/0300
datová schránka: qm4zpg4
(dále jen „**přístupovatel**“)

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

Úvodní ustanovení

1. Přístupovatel prohlašuje, že zřízení a provoz vzdálených přístupů je pro něj nutným předpokladem pro řádné provádění podpory, údržby, aktualizací, upgradů či servisu zařízení, systémů, přístrojů či aplikací spravovaných přístupovatelem, 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 zřízených vzdálených přístupů k provádění činností uvedených v této Smlouvě.
2. 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 přístupovateli umožní omezený počet vzdálených přístupů v rozsahu nezbytně nutném (dále jako „**vzdálený přístup**“ nebo též „**vzdálené přístupy**“) 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 práv a povinností smluvních stran sjednaných mezi smluvními stranami na základě jiné smlouvy, resp. smluv.
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, 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. technické 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 jiné smlouvy, resp. smluv uzavřených s přístupovatelem, jejichž předmět plnění se týká provádění činností vzdálené správy, 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, přičemž FNB tímto výslovně přístupovateli zakazuje jej dále převádět na jinou osobu či osoby, ať již právnické nebo fyzické, není-li dále stanoveno jinak. V případě, že ze smluv uzavřených mezi FNB a přístupovatelem vyplývá oprávnění pro poddodavatele, resp. subdodavatele realizovat, a tedy podílet se na plnění částí předmětu plnění z těchto smluv 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.

2. Veškeré technologie umístěné ve 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.
3. Přístupovatel se zavazuje, že vzdálený přístup do DS FNB bude iniciovat pouze ze zařízení, které je dostatečně zabezpečené, tj.:
 - a) má instalováno a pravidelně aktualizováno programové vybavení (software) na ochranu proti škodlivému software,
 - b) má instalováno pouze takové programové vybavení (software), který bylo instalováno v souladu s licenčními podmínkami autora daného programového vybavení (software),
 - c) je chráněno heslem,
 - d) má aktivní šifrování datového úložiště a pravidelně aktualizovaný operační systém,
 - e) má aktivní funkci automatického uzamknutí v případě nečinnosti.

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

4. Přístupovatel se zavazuje, že vzdálený přístup do DS FNB bude využívat jen za účelem uvedeným ve smlouvách (viz čl. 1 odst. 1 Smlouvy), resp. dle podmínek v nich sjednaných. 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.
5. Přístupovatel je povinen vždy na začátku kalendářního měsíce sdělit e-mailem na adresu admin@bulovka.cz sumář připojení v předchozím měsíci s popisem důvodu vstupu a prováděných činností. Jakékoliv nezaslání sumáře ve lhůtě do 3 pracovních dnů od začátku nového měsíce, je považováno za porušení této Smlouvy. Bude-li se toto porušení povinností ze strany přístupovatele opakovat min. ve třech případech, zakládá to právo FNB od této Smlouvy okamžitě odstoupit.
6. Dále je přístupovatel povinen zajistit, že veškeré technické prostředky jím využité 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 kontakty FNB uvedené v odst. 11 tohoto článku Smlouvy.
7. 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.
8. 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, systémům, přístrojům či aplikacím, 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 ve smlouvách, konkrétně správy, servisu, upgrade, testování, implementace. 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.

9. Přístupovatel je povinen dodržovat při plnění Smlouvy veškerou aktuální bezpečnostní politiku a předpisy FNB, které mu byly FNB předány nebo se kterými byl FNB seznámen a které mají dopad na plnění přístupovatele dle této Smlouvy. Bezpečnostní politikou a předpisy FNB, které mají dopad na plnění přístupovatele dle této Smlouvy, se rozumí bezpečnostní dokumentace, která se vztahuje k plnění přístupovatele dle této Smlouvy nebo se obvykle vztahuje k povinnostem subjektů, které jsou v dodavatelském vztahu k FNB, s přihlédnutím ke skutečnosti, že FNB je správcem a provozovatelem informačního systému základní služby. FNB je povinen přístupovateli předat nebo přístupovatele seznámit s aktuální bezpečnostní politikou a předpisy FNB, které mají dopad na plnění Poskytovatele dle této Smlouvy, o čemž bude vždy vyhotoven zápis podepsaný oběma smluvními stranami.
10. 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. 2.
11. V případě oznamování přístupu do DS FNB dle odstavce 5. 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 prostřednictvím dále uvedených kontaktních údajů smluvních stran.
 - a) Kontaktní údaje FNB:
e-mail: **xxx xxx xxx** (aktivní v časech od 7.00 – 15.30 hod.), resp.
xxx xxx xxx (aktivní v časech mezi 15:30 až 7:00 hodinou následujícího dne)
 - b) Kontaktní údaje přístupovatele:
e-mail: **xxx xxx xxx** telefon: **xxx xxx xxx**(od: 9 do: 15).
12. 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.
13. Porušení smluvních povinností přístupovatele stanovených v tomto článku Smlouvy zakládá právo FNB od Smlouvy kdykoli odstoupit.
14. 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.
15. 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 čl. 3 odst. 3, 4 nebo 9 Smlouvy, je přístupovatel povinen uhradit FNB smluvní pokutu ve výši 1 000 Kč (slovy: jeden tisíc korun českých), a to za každý jednotlivý případ porušení některé z výše uvedených povinností.

2. V případě porušení jakékoli povinností přístupovatele uvedené v čl. 3 odst. 8 Smlouvy je přístupovatel povinen uhradit FNB smluvní pokutu ve výši 5 000 Kč (slovy: pět tisíc korun českých) za každý jednotlivý případ porušení této povinnosti.
3. Smluvní pokuty dle tohoto článku jsou splatné ve lhůtě 14 dnů ode dne, kdy FNB vyzve přístupovatele 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 dvou měsíců, 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 všech smluv sjednaných s přístupovatelem, jejichž předmět plnění se týká provádění činností vzdálené správy, a který současně vyžaduje zřízení a provoz vzdáleného přístupu 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. 11 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 nejvěrněji 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. 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

10. Tato Smlouva je vyhotovena ve dvou stejnopisech s platností originálu. Každá ze smluvních stran obdrží po jednom stejnopisu této Smlouvy, jež má platnost originálu.

11. Smluvní strany si před podpisem tuto Smlouvu řádně přečetly a svůj souhlas s obsahem jejích jednotlivých ustanovení stvrzují svým podpisem.

V Praze dne 30.5.2025

elektronicky podepsáno



.....

Mgr. et Mgr. Jan Alexa

náměstek pro informační a komunikační
technologie,

na základě pověření

Fakultní nemocnice Bulovka

V dne 3.6.2025

elektronicky podepsáno



.....

RNDr. Václav Vohánka

jednatel

Sefima s.r.o.

Příloha č.1

Zde budou uvedeny všechny VPN přístupy přístupovatele platné ke dni podpisu Smlouvy, včetně e-mailů zaměstnanců s přístupem.

xxx xxx xxx

BEZPEČNOSTNÍ DOPORUČENÍ NUKIB 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 DOMÉNY NA ÚROVNI GATEWAY (BLACKLISTY).

NASAĎTE 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

záznamy kritických pracovních stanic a serverů a provoz překračující perimetr sítě pro případné forenzní zkoumání po průniku do sítě a systému. 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 výhlásek je minimální lhůta 18 měsíců. V případě sítí strategického významu zvážte i možnost automaticky aktivovaného píného 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 blokuje 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 ideálním případě 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 blokových) a okamžitým automatickým vyhodnocením a uložením po dobu minimálně 18 měsíců, více podle místních okolností a významu sítě.

APLIKUJTE WHITELISTING WEBOVÝCH DOMÉN

(povolených a blokových) a okamžitým automatickým vyhodnocením a uložením po dobu minimálně 18 měsíců, více podle místních okolností a významu sítě.

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 nasaďte na kompletní IP rozsahy vaší organizace.

VYPRACUJTE DISASTER RECOVERY PLAN (DRP)

a mějte připravené správné a funkční emailové adresy a telefonní čísla na ostatní administrátory, nasazené 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 neaktualizovaného softwaru proveďte v rámci možnosti 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 funkcionality, 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 IDSIPS 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 persistence a další.

ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ

(povolených a blokových) a okamžitým automatickým vyhodnocením 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 PROPOUŠŤEJTE POUZE RELEVANTNÍ DRUHY PŘÍLOH

– po důkladné analýze chování uživatelů určete typy souborů, které potřebují poslat e-mailem. Ostatní formáty příloh blokuje – především spuštění skriptů. Dále ověřte 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 spítní 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 spouštění 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 jim 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 otku klíče se serverem, kde je použitý, využijte SSHFP záznamy v DNS ideálně v kombinaci s DNSSEC, který zajistí autenticitu odpovědi obsahující SSHFP záznam.

PROVÁDĚJTE HARDENING KONFIGURACE SERVEROVÝCH APLIKACÍ

tj. databázi, 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.

VYNUTTE 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 OPRAVNĚNÍ

a nastavte jednotnou bezpečnostní politiku. Účtům, u kterých to není vyžadováno, odeberte rozšířená oprávnění a zakažte spuštění 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 nepřivilegovaný účet. Účet s oprávněním doménového administrátora je použit pouze ke správě Domain Controlleru (tzn. nepřistupuje na klientské stanice a servery).

PŘIDĚLTE KAŽDÉMU ADMINISTRÁTORŮVI 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).

VYNUTTE POUŽÍVÁNÍ SILNÝCH HESEL

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

PRAVIDELNĚ KONTROLUJTE UŽIVATELSKÉ ÚČTY A JEJICH OPRAVNĚNÍ

a to jak lokální, tak centrálně spravované.

