Docusign Envelope ID: F095EE93-D534-810F-804D-F300DFA9737E

Nemocnice Plzeňského kraje | Domažlice | Horažďovice Klatovy | Rokycany Stod | Svatá Anna

Minimální bezpečnostní požadavky na dodávky a služby ICT / OT / zdravotnických zařízení

Požadavky představují minimální bezpečnostní standard, který je povinen dodavatel splnit při dodávce ICT/OT technologií, softwaru, hardwaru, technologických a zdravotnických zařízení, komponent, podpory nebo souvisejících služeb, pokud se řešení připojuje do ICT/OT infrastruktury, komunikuje s ní, nebo zpracovává data, jejichž vlastníkem je jakýkoliv subjekt, jenž je součástí skupiny Nemocnice Plzeňského kraje (dále jen NPK).

1 Řízení přístupu dodavatele, technických změn a bezpečnostních událostí

- Do ICT/OT infrastruktury NPK se lze připojovat pouze schváleným a řízeným způsobem, zejména prostřednictvím VPN nebo jiného technického řešení určeného NPK. Není akceptováno použití nástroje pro neautorizovaný vzdálený přístup dodavatele.

- K prostředkům NPK lze připojovat pouze pracovní stanice a zařízení, u kterých je výrobcem zajištěna technická podpora a dostupnost bezpečnostních aktualizací, která jsou vybavena ochranou proti škodlivému kódu a jsou aplikována opatření znemožňující zneužití a neoprávněnou manipulaci.

- Vzdálený přístup je vždy veden na jméno konkrétní osoby/pracovníka dodavatele. Sdílené účty, obecné účty nebo anonymní přístupy nejsou přípustné, pokud oddělení bezpečnost a organizace řízení (dále jen BOŘ) NPK písemně neschválí výjimku pro specifický technický účel.

- Je vyžadováno, aby přidělená oprávnění odpovídala zásadám least privileged, need-to-know a just-in-time. Dodavatel je povinen používat pouze taková oprávnění, která jsou nezbytná pro plnění smluvního účelu.

- První přihlášení do systému nebo relace probíhá pod jmenným neprivilegovaným účtem; privilegované oprávnění lze použít až následně a jen po dobu nezbytně nutnou k provedení schválené činnosti.

Docusign Envelope ID: F095EE93-D534-810F-804D-F300DFA9737E

- Dodavatel je povinen před zahájením plnění sdělit NPK prostřednictvím formuláře pro dodavatele technické a komunikační požadavky řešení, a to zejména kontakty, popis dodávaného řešení, vazby na další systémy, seznam hlavních komponent (struktura komunikace např. čtečka -> gateway -> server), náležitosti síťové komunikace, jako jsou protokoly, porty aj. uvedené v příslušném formuláři, technologie specifické pro nasazované řešení, jako nestandardní síťové protokoly apod., DNS záznamy, HW nároky, uživatelské a systémové účty a jejich potřebná oprávnění, frekvenci, způsob a velikost záloh, činnosti související s údržbou dodávaného řešení, rozsah správy a podpory, rozsah školení, je-li součástí implementace, případně jiné požadavky uvedené ve formuláři pro dodavatele.

- Dodavatel je povinen předem oznamovat plánované servisní zásahy, změny konfigurace, aktualizace, nasazení verzí a jiné technické zásahy, které mohou mít dopad na bezpečnost, dostupnost, integritu nebo auditovatelnost řešení.

- Jakákoli změna řešení, která může ovlivnit síťovou komunikaci, vazby identit, logování, oprávnění, způsob ukládání dat, šifrování, správu zranitelností nebo bezpečnostní architekturu, podléhá předchozímu oznámení a případně schválení oddělením BOŘ NPK.

- Dodavatel je povinen bez zbytečného odkladu oznamovat bezpečnostní incident, bezpečnostní událost nebo jinou nežádoucí bezpečnostní situaci, která má nebo může mít dopad na plnění pro NPK, na integritu dat, na ICT/OT infrastrukturu NPK nebo dodaného řešení. Oznámení obsahuje popis situace, čas zjištění, dotčená aktiva, předběžný dopad a kontaktní osobu dodavatele.

- Po ukončení potřeby přístupu pracovníka dodavatele k aktivům NPK, ať už z důvodu ukončení smluvního vztahu, ukončení pracovního poměru, nebo potřeby přístupu osoby dodavatel bezodkladně požádá o zrušení nebo blokaci přístupu. Pokud není dohodnuto jinak, dodavatel tak učiní nejpozději do 24 hodin od vzniku této skutečnosti.

- Dodavatel bez předchozího písemného schválení odpovědným zástupcem NPK nezapojí do plnění třetí stranu, nepropojuje technologické řešení s jiným prostředím, nepřesouvá data NPK mimo schválené prostředí a také nezřizuje neodsouhlasené kopie, exporty nebo zálohy dat.

- Dodavatel je povinen spolupracovat s NPK při bezpečnostním testování dodávaného řešení a poskytnout veškeré podklady, které jsou k testování nezbytné.

Docusign Envelope ID: F095EE93-D534-810F-804D-F300DFA9737E

- Testovací nebo servisní účty zřízené pro účely skenování, podpory nebo diagnostiky mají úroveň přístupových oprávnění a rozsah přístupu na nezbytné minimum, jsou auditovatelné, aktivované jen po dobu potřeby a po ukončení činnosti jsou zrušené nebo deaktivované.

- Po skončení smluvního vztahu nebo po ukončení konkrétního plnění je dodavatel povinen podle pokynu NPK vrátit, bezpečně předat, převést nebo prokazatelně zničit data, přístupové údaje, nosiče a další informace nebo artefakty, které v souvislosti s plněním získal nebo vytvořil.

- Zařízení, software ani komponenty neobsahují nezdokumentované administrátorské účty, hardcoded přístupové údaje, neodsouhlasené vzdálené přístupy, výchozí hesla, nezdokumentované integrační vazby nebo jiné skryté mechanismy umožňující obcházení bezpečnostních kontrol.

1.1 Postup pro nahlášení incidentu nebo jiné nežádoucí situace

- Dodavatel oznámí zjištěnou situaci bez zbytečného odkladu NPK prostřednictvím Servicedesku na adrese https://sd.nemocnicepk.cz nebo v naléhavých případech i telefonicky IT pohotovosti na tel. 778 728 341

- Oznámení obsahuje alespoň: stručný popis, datum a čas zjištění, dotčené systémy nebo data, přijatá okamžitá opatření, předpokládaný dopad a kontaktní osobu odpovědnou za další koordinaci.

- Dodavatel je povinen poskytnout součinnost při šetření, zajištění důkazů, obnově provozu systému nebo zařízení a při realizaci nápravných a preventivních opatření.

1.2 Postup pro zřízení a správu uživatelských účtů

- Žádosti o zřízení přístupu obsahují identifikaci osoby, účel přístupu, rozsah požadovaných oprávnění, dobu potřebnosti a vazbu na konkrétní smluvní plnění.

- Účty se zřizují pouze po schválení oddělením BOŘ NPK.

- Dodavatel odpovídá za aktuálnost údajů o svých pracovnících a za okamžité oznámení změn, které mají vliv na oprávněnost přístupu.

Docusign Envelope ID: F095EE93-D534-810F-804D-F300DFA9737E

- Dodavatel je povinen pro přístup do prostředí NPK přistupovat pomocí vyhrazeného správcovského prostředí. Administrátorské účty budou vedeny odděleně pro každého uživatele, přístupy mohou být časově ohraničeny.

2 Bezpečnostní politiky a organizační požadavky

2.1 Organizace bezpečnosti

- Bezpečnostní koordinace mezi NPK a dodavatelem probíhá prostřednictvím určených oprávněných osob.
- Pro dodané řešení je na straně dodavatele určena odpovědná osoba za provoz, správu přístupů, změny, bezpečnostní incidenty, aktualizace.
- Dodavatel je povinen akceptovat bezpečnostní politiky, standardy, provozní pravidla a technické podmínky NPK vztahující se k poskytovanému plnění.

2.2 Řízení přístupu k informacím a systémům

- NPK má aplikován formální postup pro vytvoření, změnu, přezkum a zrušení přístupových práv.
- Přidělování a používání vyšších oprávnění je řízeno, odůvodněno a průběžně přezkoumáváno.
- Každý uživatelský účet dodavatele je zpracován v rámci těchto procesů.
- Každý uživatel dodavatele má jedinečný identifikátor ve formě jmenného účtu. Sdílené identity lze použít jen po schválení oddělením BOŘ NPK.
- Hesla a jiné autentizační prostředky jsou spravovány řízeným procesem; dodavatel je povinen chránit je proti zneužití, zpřístupnění a neautorizovanému sdílení.
- Použití nástrojů schopných překonat systémové nebo aplikační kontroly je schválené oddělením BOŘ NPK a je auditovatelné, omezené na autorizované osoby a řádně zdůvodněné.

2.3 Monitorování, logování a auditní záznamy

- Je vyžadováno, aby relevantní bezpečnostní a provozní události byly zaznamenávány, chráněny proti neoprávněné manipulaci a vyhodnocovány přiměřeně povaze řešení.

Docusign Envelope ID: F095EE93-D534-810F-804D-F300DFA9737E

- Zaznamenávány jsou zejména přihlášení, neúspěšná přihlášení, použití privilegovaných účtů, změny účtů a oprávnění, bezpečnostně významné změny konfigurace, události související s přístupem k datům a pokusy o obcházení kontrol.
- Je-li to technicky možné a NPK toto vyžaduje, jsou záznamy předávány centralizovaně nebo jinak zpřístupněny pro bezpečnostní dohled NPK.
- Zařízení a systémy mají správně synchronizovaný čas, aby auditní záznamy byly použitelné pro korelaci a vyšetřování.

3 Doplňující bezpečnostní požadavky pro software, servis a outsourcing

3.1 Používání privilegovaných programů a nástrojů

- Použití systémových utilit, administrátorských nástrojů a servisních mechanismů je omezeno na autorizované osoby a odůvodněné činnosti v rámci smluvního plnění. Použití schvaluje oddělení BOŘ NPK.
- Tyto nástroje jsou odděleny od běžného uživatelského používání, chráněny odpovídající autentizací a jejich použití má být evidováno.
- Nepotřebné utility, výchozí účty a zbytečný systémový software jsou odstraněny nebo bezpečně zakázány.
- Bezpečnostní parametry operačních systémů, aplikací a zařízení jsou nastaveny v souladu s minimální bezpečnostní úrovní NPK a doporučeními výrobce.

3.2 Outsourcing a zapojení třetích stran

- Pokud dodavatel využívá poddodavatele nebo jinou třetí stranu, je tato skutečnost předem oznámena a schválena NPK.
- Dodavatel odpovídá za to, že zapojené třetí strany budou vázány alespoň stejným rozsahem bezpečnostních povinností, jaké platí pro dodavatele.

Docusign Envelope ID: F095EE93-D534-810F-804D-F300DFA9737E

- V rámci smluvního vztahu je řešena důvěrnost, integrita a dostupnost informací, omezení přístupu, hlášení incidentů, řízení změn, součinnost při auditu, kontinuita činností a bezpečné ukončení služby.

3.3 Cloudové služby

- Využití cloudových služeb podléhá předchozímu posouzení vhodnosti, rizik a souladu s požadavky NPK.
- Bez předchozího schválení nejsou v cloudových službách zpracovávána nebo ukládána data NPK, zejména pokud jde o citlivá, neveřejná, osobní nebo provozně významná data.
- Smluvní a technické podmínky cloudové služby řeší minimálně umístění dat, řízení přístupu, šifrování, logování, oznamování změn, zapojení subdodavatelů a ukončení služby.

3.4 Odpovědnost třetích stran

- Dodavatel a všechny osoby jednající jeho jménem jsou povinni chránit informační aktiva NPK a dodržovat stanovené bezpečnostní požadavky po celou dobu trvání smluvního vztahu.
- Požadavky na fyzickou a logickou bezpečnost jsou posouzeny před zahájením plnění a přiměřeně promítnuty do smluvního vztahu, technického řešení a provozních pravidel.
- Po ukončení smluvního vztahu jsou citlivé a neveřejné informace vráceny, předány, bezpečně vymazány nebo zničeny; NPK může požadovat písemné potvrzení o provedení tohoto kroku.

3.5 Bezpečnostní požadavky na informační systémy

- U nově vytvořeného nebo významně upravovaného řešení jsou bezpečnostní požadavky zohledněny již ve fázi návrhu, specifikace, vývoje, testování, nasazení a údržby.
- Dodavatel je povinen zohlednit řízení zranitelností, bezpečné výchozí nastavení, správu konfigurace, oddělení prostředí, ochranu dat, logování a možnost bezpečné aktualizace.
- Pro výměnu informací a dat mají být používány schválené a chráněné komunikační kanály; veřejné nebo neřízené služby nejsou používány.

Docusign Envelope ID: F095EE93-D534-810F-804D-F300DFA9737E

3.6 Zabezpečení aplikačních služeb ve veřejných sítích

- Je vyžadováno, aby řešení poskytovaná přes veřejné sítě byla přístupná pouze přes schválenou síťovou a bezpečnostní infrastrukturu NPK nebo jinak schválený bezpečný mechanismus.
- Dodavatel neobchází bezpečnostní kontroly NPK prostřednictvím neřízeného mobilního připojení, ad hoc tunelů, neschválených Wi-Fi sítí nebo jiných alternativních cest.
- Publikované služby jsou navrženy a provozovány tak, aby nedocházelo k neautorizovanému zveřejnění dat, změně obsahu, zneužití transakcí nebo poškození dobrého jména NPK.

3.7 Zálohování

- Pokud je součástí plnění ukládání nebo správa dat NPK, je zajištěno přiměřené zálohování, ochrana záloh a možnost obnovy.
- Zálohy nejsou mazány, uchovávány a přesouvány mimo schválené prostředí bez vědomí NPK.
- Na vyžádání dodavatel doloží, jak je řešena obnova dat a nakládání se zálohami.

4 Požadavky bezpečnostního testování software

Tyto požadavky představují minimální rámec bezpečnostního ověření software, webových aplikací, API, integračních komponent a souvisejících služeb před nasazením do produkčního prostředí a při významných změnách.

- Statická analýza kódu (SAST): provést kontrolu zdrojového kódu vhodným nástrojem nebo a vyhodnotit nalezené zranitelnosti a bezpečnostní chyby.
- Dynamická analýza (DAST): otestovat aplikaci v testovacím prostředí a ověřit odolnost vůči hrozbám z aktuálního vydání standardu OWASP TOP 10. Dodavatel ručí za to, že každý build webové aplikace určený pro distribuci do produkčního prostředí projde testováním nástrojem OWASP ZAP a neobsahuje zranitelnost s hodnocením vyšším než "low".
- Testování vstupů a výstupů: ověřit validaci vstupů, zpracování hraničních a neplatných hodnot a ochranu citlivých dat ve výstupech.

Docusign Envelope ID: F095EE93-D534-810F-804D-F300DFA9737E

- Ověření autentifikace a autorizace: potvrdit, že citlivé funkce, data a administrační rozhraní jsou přístupné pouze oprávněným objektům a že nelze neoprávněně eskalovat oprávnění.

- Testování šifrování a přenosů dat: ověřit bezpečnost použitých kryptografických algoritmů a ochranu citlivých údajů při přenosu a ukládání.

- Dependency a library scan: identifikovat používané komponenty a knihovny, vyhodnotit známé zranitelnosti a případně je odstranit nebo odůvodnit jejich akceptaci.

- Logování: ověřit, že logy neobsahují citlivá data, jsou chráněny před manipulací a neumožňují zneužití typu log injection nebo obdobné útoky.

- Testování API bezpečnosti: ověřit objektovou autorizaci, CORS, SSRF, rate limiting a další běžně zneužívané zranitelnosti. K testování bezpečnosti API může dodavatel využít některý z doporučených nástrojů společností OWASP, uvedených na tomto odkaze: https://owasp.org/www-community/api_security_tools

- Dodavatel je povinen před předáním předmětu smlouvy odstranit všechny zranitelnosti klasifikované jako kritické a vysoké. Zranitelnosti střední závažnosti jsou zdokumentovány, odůvodněny a opatřeny plánem nápravy. Předání předmětu smlouvy bez splnění těchto podmínek se považuje za nesplnění bezpečnostních požadavků.

5 Závěrečná ustanovení

- Tento dokument stanoví minimální bezpečnostní požadavky. NPK je oprávněna podle charakteru plnění stanovit přísnější nebo doplňující požadavky.

- Pokud jsou v konkrétní smlouvě, zadávací dokumentaci, bezpečnostní příloze, návrhu architektury nebo provozním standardu NPK uvedeny přísnější požadavky, mají přednost před tímto dokumentem.

- Dodavatel bere na vědomí, že nesplnění těchto požadavků může být důvodem k vyloučení z výběrového řízení, k nepřevzetí plnění, k požadavku na nápravu nebo k uplatnění smluvních prostředků podle konkrétní smlouvy.