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

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

Níže uvedené požadavky představují minimální bezpečnostní standard, který musí dodavatel splnit při dodávce softwaru, hardwaru, zařízení, komponent, podpory nebo souvisejících služeb, pokud se řešení připojuje do podnikové sítě, komunikuje s ní nebo zpracovává data skupiny Nemocnice Plzeňského kraje (dále jen NPK).

1 Řízení přístupu dodavatele, technických změn a bezpečnostních událostí

- Do podnikové sítě NPK se lze připojovat pouze schváleným a řízeným způsobem, zejména prostřednictvím VPN nebo jiného technického řešení určeného organizací. Dodavatel nesmí použít vlastní neautorizovaný vzdálený přístup.
- K prostředkům NPK se mohou připojovat pouze pracovní stanice a zařízení, která jsou výrobcem podporována, průběžně aktualizována a vybavena ochranou proti škodlivému kódu, zneužití a neoprávněné manipulaci.
- Vzdálený přístup musí být vždy veden na jméno konkrétní fyzické osoby. Sdílené účty, obecné účty nebo anonymní přístupy nejsou přípustné, pokud zástupce NPK písemně neschválí výjimku pro specifický technický účel.
- Přidělená oprávnění musí odpovídat zásadám least privileged, need-to-know a JIT. Dodavatel je povinen používat pouze taková oprávnění, která jsou nezbytná pro plnění smluvního účelu.
- První přihlášení do systému nebo relace musí proběhnout pod jmenným neprivilegovaným účtem; privilegované oprávnění lze použít až následně a jen po dobu nezbytně nutnou k provedení schválené činnosti.
- Dodavatel je povinen před zahájením plnění sdělit organizaci technické a komunikační požadavky řešení, zejména používané porty, protokoly, směry komunikace, závislosti na externích službách, požadavky na DNS, NTP, aktualizační servery a případné integrace do internetu.

- Pokud to povaha plnění vyžaduje, musí dodavatel umožnit zaznamenávání relevantních bezpečnostních a provozních událostí a jejich předávání do log managementu nebo jiného monitorovacího řešení NPK. Rozsah, forma a způsob předávání logů bude stanoven organizací podle povahy řešení.

- 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 organizací.

- Dodavatel je povinen bez zbytečného odkladu oznamovat bezpečnostní incident, podezření na incident nebo jinou nežádoucí bezpečnostní situaci, která se týká NPK, jejích dat, její infrastruktury nebo dodaného řešení. Oznámení musí obsahovat alespoň popis situace, čas zjištění, dotčená aktiva, předběžný dopad a kontaktní osobu dodavatele.

- Po ukončení pracovního poměru, smluvního vztahu nebo potřeby přístupu osoby na straně dodavatele musí dodavatel bezodkladně požádat o zrušení nebo blokaci přístupu. Pokud není dohodnuto jinak, musí tak učinit nejpozději do 24 hodin od vzniku této skutečnosti.

- Dodavatel nesmí bez předchozího písemného schválení odpovědným zaměstnancem NPK zapojit do plnění třetí stranu, propojit řešení s dalším prostředím, přesouvat data NPK mimo schválené prostředí ani zřizovat neodsouhlasené kopie, exporty nebo zálohy dat.

- Pokud skupina NPK požaduje provádění skenování zranitelností, bezpečnostního testování nebo ověření konfigurace, je dodavatel povinen poskytnout přiměřenou součinnost, včetně technických podkladů, testovacích účtů, přístupových omezení a vyhrazeného kontaktního místa.

- Testovací nebo servisní účty zřízené pro účely skenování, podpory nebo diagnostiky musí být omezené na nezbytný rozsah, auditovatelné, aktivované jen po dobu potřeby a po ukončení činnosti 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 nesmí obsahovat 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 určenému kontaktnímu místu NPK; v naléhavých případech i telefonicky.

- Oznámení musí obsahovat 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 a při realizaci nápravných a preventivních opatření.

1.2 Postup pro zřízení a správu uživatelských účtů

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

- Účty se zřizují pouze po schválení odpovědnou osobou NPK.

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

- NPK může požadovat více faktorové ověření, oddělení administrátorských účtů, časové omezení přístupů nebo použití vyhrazeného správcovského prostředí.

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

2 Bezpečnostní politiky a organizační požadavky

2.1 Organizace bezpečnosti

- Bezpečnostní koordinace mezi organizací a dodavatelem musí probíhat prostřednictvím určených oprávněných osob.
- Pro dodané řešení musí být určeny odpovědnosti za provoz, správu přístupů, změny, bezpečnostní incidenty, aktualizace a kontakt pro eskalaci.
- Dodavatel je povinen respektovat bezpečnostní politiky, standardy, provozní pravidla a technické podmínky NPK vztahující se k poskytovanému plnění.

2.2 Řízení přístupu k informacím a systémům

- Musí existovat formální postup pro vytvoření, změnu, přezkum a zrušení přístupových práv.
- Přidělování a používání privilegií musí být řízeno, odůvodněno a průběžně přezkoumáváno.
- Každý uživatel musí mít jedinečný identifikátor; sdílené identity lze použít jen výjimečně, s evidencí odpovědných osob a s výslovným schválením zaměstnancem NPK.
- Hesla a jiné autentizační prostředky musí být spravovány řízeným procesem; dodavatel je povinen chránit je proti zneužití, zpřístupnění a neautorizovanému sdílení.
- Použití nástrojů schopných obejít systémové nebo aplikační kontroly musí být auditovatelné, omezené na autorizované osoby a zdůvodněné.

2.3 Monitorování, logování a auditní záznamy

- Relevantní bezpečnostní a provozní události musí být zaznamenávány, chráněny proti neoprávněné manipulaci a vyhodnocovány přiměřeně povaze řešení.
- Zaznamenávány musí být 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 organizací vyžadované, musí být záznamy předávány centralizovaně nebo jinak zpřístupněny pro bezpečnostní dohled.

- Zařízení a systémy musí mít 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 musí být omezeno na autorizované osoby a odůvodněné činností v rámci smluvního plnění.
- Tyto nástroje musí být odděleny od běžného uživatelského používání, musí být chráněny odpovídající autentizací a jejich použití má být evidováno.
- Nepotřebné utility, výchozí účty a zbytečný systémový software musí být odstraněny nebo bezpečně zakázány.
- Bezpečnostní parametry operačních systémů, aplikací a zařízení musí být 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, musí být tato skutečnost předem oznámena a schválena organizací, pokud to skupina NPK požaduje.
- Dodavatel odpovídá za to, že zapojené třetí strany budou vázány alespoň stejným rozsahem bezpečnostních povinností, jaké platí pro dodavatele.
- V rámci smluvního vztahu musí být řešena důvěrnost, integrita a dostupnost informací, omezení fyzického a logického přístupu, hlášení incidentů, řízení změn, právo na 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 nesmí být 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 musí řešit alespoň 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 musí být posouzeny před zahájením plnění a přiměřeně promítnuty do smluvního vztahu, technického řešení a provozních pravidel.
- Po ukončení smluvního vztahu musí být citlivé a neveřejné informace vráceny, předány, bezpečně vymazány nebo zničeny; skupina NPK může požadovat písemné potvrzení o provedení tohoto kroku.

3.5 Bezpečnostní požadavky na informační systémy

- U nově vytvářeného nebo významně upravovaného řešení musí být 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 nesmí být použity bez schválení zaměstnancem NPK.

3.6 Zabezpečení aplikačních služeb ve veřejných sítích

- Řešení poskytovaná přes veřejné sítě musí být přístupná pouze přes schválenou síťovou a bezpečnostní infrastrukturu NPK nebo jinak schválený bezpečný mechanismus.
- Dodavatel nesmí obcházet bezpečnostní kontroly NPK prostřednictvím neřízeného mobilního připojení, ad hoc tunelů, neschválených Wi-Fi sítí nebo jiných alternativních cest.

- Publikované služby musí být navrženy a provozovány tak, aby nedocházelo k neautorizovanému zveřejnění dat, změně obsahu, zneužití transakcí nebo poškození dobrého jména NPK.

3.7 Ochrana transakcí aplikačních služeb

- Transakce musí být chráněny odpovídající identifikací a autentizací účastníků, řízením oprávnění a šifrováním komunikace.
- Musí být zajištěna auditovatelnost transakcí a ochrana záznamů proti neoprávněnému přístupu, změně nebo ztrátě.
- Úložiště detailních záznamů o transakcích nesmí být volně přístupná a musí podléhat odpovídajícímu řízení přístupu.

3.8 Zálohování

- Pokud je součástí plnění ukládání nebo správa dat NPK, musí být zajištěno přiměřené zálohování, ochrana záloh a možnost obnovy.
- Zálohy nesmí být vytvářeny, uchovávány ani přesouvány mimo schválené prostředí nebo bez vědomí NPK.
- Na vyžádání musí dodavatel doložit, jak je řešena obnova, konzistence dat a bezpečné nakládání se zálohami.

4 Požadavky bezpečnostního testování software

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

- Statická analýza kódu (SAST): provést kontrolu zdrojového kódu vhodným nástrojem nebo ekvivalentním postupem a vyhodnotit nalezené zranitelnosti a bezpečnostní chyby.

- Dynamická analýza (DAST): otestovat aplikaci v testovacím nebo jinak řízeném prostředí a ověřit odolnost vůči běžným webovým a aplikačním hrozbám, včetně kategorií odpovídajících aktuálně uznávaným standardům. 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, bezpečnost chybových hlášení a ochranu citlivých dat ve výstupech.

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

- Testování šifrování a přenosů dat: ověřit bezpečné komunikační protokoly, vhodnost použitých kryptografických mechanismů a ochranu citlivých údajů při přenosu i ukládání.

- Správa credentials a tajemství: ověřit, že řešení neobsahuje hardcoded přístupové údaje a že tajemství jsou ukládána, předávána a obnovována řízeným a bezpečným způsobem.

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

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

- Testování API bezpečnosti: ověřit správu identit a relací, objektovou a funkční autorizaci, CORS, SSRF, rate limiting, ochranu proti zneužití rozhraní a bezpečnost integračních vazeb aj.

- Dodavatel je povinen před předáním předmětu smlouvy odstranit všechny zranitelnosti klasifikované jako kritické a vysoké. Zranitelnosti střední závažnosti musí být 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. Skupina NPK je oprávněna podle charakteru plnění stanovit přísnější nebo doplňující požadavky.

- Pokud jsou v konkrétní smlouvě, zadávací dokumentaci, bezpečnostní příloze, architekturním návrhu 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.