PRAVIDLA MINIMÁLNÍ KYBERNETICKÉ BEZPEČNOSTI PRO DODAVATELE

Uherskohradišťská nemocnice a.s.

Obsah

1 Úvodní ustanovení

1. **Pravidla minimální kybernetické bezpečnosti pro dodavatele** Uherskohradišťské nemocnice a.s. (dále též UHN) tvoří soubor závazných pravidel a postupů vymezujících způsob a požadovanou úroveň kybernetické bezpečnosti, vymezení aktiv (aktivum je cokoliv, co má hodnotu pro organizaci) a způsob jejich ochrany, týkající se firem a organizací se smluvním vztahem k UHN.
2. Dodržování pravidel uvedených v tomto dokumentu je povinné pro všechny smluvní partnery UHN, kterých se dotýká problematika kybernetické bezpečnosti.
3. Používané i nově zaváděné informační systémy v rámci UHN musí být upraveny, vyvíjeny a vybírány a spravovány tak, aby splňovaly zásady kybernetické bezpečnosti podle tohoto dokumentu.

1.1 Cíle dokumentu

1. Kybernetická bezpečnost (dále také „***KB***“) je ochrana elektronických informací, systémů a služeb proti živelním událostem, lidským omylům a úmyslné manipulaci s cílem snížit pravděpodobnost a dopad bezpečnostních incidentů na minimum.
2. Cílem Pravidel **minimální bezpečnosti pro dodavatele** s UHN je obecně:
   a) specifikovat jasné zásady KB pro dodavatele UHN
   b) zabránit neautorizovanému přístupu k informacím UHN,
   c) umožnit provádění kontroly přístupu k informacím,
   d) zajistit dostupnost informací pro oprávněné uživatele i procesy,
   e) zabránit neautorizované modifikaci či zneužití dat nebo jiných aktiv a umožnit ověření původu informací,
   f) definovat základní pravidla rozvoje a výběru nových používaných prostředků a technologií (vývoj zabezpečovacích prostředků, vlastnosti používaných aplikací a operačních systémů),

2 Obecné povinnosti

Mezi povinnosti smluvních partnerů patří zejména:

a) používání informačních aktiv s UHN pouze v souladu s rozsahem přístupových oprávnění a pouze ke schváleným účelům,

b) zajištění ochrany svých autentizačních údajů, (login, heslo, identifikační předmět)

c) odpovědnost za každý přístup k informacím, provedený prostřednictvím jejich autentizačních údajů,

d) respektování všech bezpečnostních opatření a procedur určených vlastníkem informací,

e) nerozšiřování dat bez souhlasu vlastníka informací.

3 Bezpečnost HW, SW a komunikace

Smluvní partneři UHN musí chránit aktiva UHN, která používají ke své práci či výkonu pro UHN, a zabránit jejich poškození, zneužití nebo odcizení.

3.1 Pracovní stanice, notebooky

Při práci na koncových uživatelských pracovištích UHN musí být splněny nejméně následující bezpečnostní zásady:

a) použití počítače UHN je umožněno pouze oprávněné osobě,

b) je zakázáno připojovat vlastní počítače do vnitřní sítě UHN bez vědomí managera kybernetické bezpečnosti nebo vedoucího útvaru Informační a komunikační technologie,

c) pracovní stanice nesmí být ponechány bez dozoru zapnuté a s přihlášeným uživatelem. Je třeba přinejmenším použít heslem chráněného spořiče obrazovky,

d) počítač smluvního partnera, který má být připojen do vnitřní sítě UHN, musí mít instalován a spuštěn systém pro ochranu před škodlivými programy (antivirový program) v nejnovější verzi programu i virové databáze,

e) smluvní partner je povinen chránit vybavení UHN, udržovat okolo sebe bezpečné pracovní prostředí,

f) v případě ukončení práce se zařízením je smluvní partner povinen provést odhlášení od systému, aby se zamezilo zneužití jeho přístupových práv.

3.2 Využívání internetu

1. Systémy v UHN vztahující se k počítačové síti, internetu a intranetu, včetně počítačového vybavení, programů, operačních systémů, medií pro ukládání dat, schránek elektronické pošty UHN, možností prohlížení internetových stránek a zdrojů přístupných na datových úložištích jsou vlastnictvím UHN.
2. Zaměstnanci smluvních partnerů mají dovoleno používat internetové připojení do a z vnitřní sítě UHN pouze za účelem činnosti pro UHN. Způsob připojení do vnitřní sítě UHN a autentizace musí být předem dohodnut s manažerem kybernetické bezpečnosti, vedoucím útvaru Informační a komunikační technologie UHN, nebo jím pověřeným pracovníkem odboru IT. Obecně musí platit povinnost oznámit předem datum a čas přihlášení k vnitřnímu prostředí a následně ukončení práce ve vnitřním prostředí UHN.
   Pozn: Do „vnitřní sítě nemocnice“ nespadá připojení přes volnou wifi, poskytovanou UHN pacientům.

4 KB systémů IT

U vyvíjených, dodávaných a spravovaných informačních systémů musí být zajištěno dodržení níže uvedených povinností.

4.1 Používání hesel

a) Aplikace musí být vytvářeny tak, aby znemožnily přístup bez zadání hesla.

b) Aplikace musí být schopná ověřovat uživatele v Microsoft AD. Používání lokálních účtů v aplikaci je možné jen po odsouhlasení manažerem KB nebo vedoucím odboru IT. U svých lokálních uživatelů musí aplikace dodržovat následující pravidla:

c) Uživatel aplikace musí být nucen si heslo pravidelně měnit.

d) Aplikace musí být vytvořena tak, aby byl počet neúspěšných pokusů o přihlášení omezen. Po třech neúspěšných pokusech o přihlášení musí být další zadávání dočasně ochromeno nebo spojení rozpojeno.

e) Pokud je při přihlašování do aplikace některá část zadaných informací chybná, nesmí být uživateli poskytnuta informace, ve kterém z údajů je chyba.

f) V případě, že je povolen přístup do aplikace, v níž určuje vstupní heslo administrátor, je povinností autora aplikace vynutit si změnu tohoto inicializačního hesla.

g) Všichni uživatelé musí při své činnosti užívat jedinečný identifikátor (přihlašovací jméno) tak, aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činnosti.

h) Zaměstnanci dodavatele smí používat jedno přihlašovací jméno pro několik svých zaměstnanců, přičemž dodavatel odpovídá za veškeré úkony provedené v informačním systému UHN pod těmito identifikátory.

4.2 Monitorování používání a přístupu k systému

V informačních systémech musí být pořizovány auditní záznamy obsahující minimálně:

a) identifikaci uživatele,

b) datum a čas přihlášení a odhlášení,

c) identifikaci místa, odkud se uživatel přihlašoval (pokud je to možné),

d) záznamy o přístupu (o úspěšném i neúspěšném pokusu o přihlášení).

Auditní záznamy musí být pořizovány tak, aby bylo možné jejich automatické sledování a vyhodnocování.

4.3 Řízení přístupu k informačnímu systému

a) Před umožněním přístupu musí být každý uživatel identifikován a autentizován.

b) Informační systém by měl po určité době nečinnosti uživatele (doporučeno 15 minut) tohoto uživatele odhlásit.

c) Po určitém množství neúspěšných autentizačních pokusů (doporučeno 3) se musí ukončit přihlašovací procedura.

d) V případě neúspěšné autentizace nesmí systém poskytnout uživateli informaci o tom, která část autentizace je chybná.

e) Pro každého uživatele systému musí být možno identifikovat, jaká má přístupová práva.

f) Pro každý informační systém musí být možno vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto prostředku s rozlišením druhu přístupových práv (čtení, úprava atd.)

g) Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo skupině.

5 Bezpečnost dat

5.1 Data vstupující do IS UHN

Data vstupující do systémů UHN musí být kontrolována, aby byla zajištěna jejich správnost. V aplikacích se musí evidovat identifikátor uživatele nebo procesu, který změny nebo pořízení provedl.

Pro kontrolu dat je nezbytné aplikovat opatření:

a) Vstupní kontrola (neplatné znaky, rozsah, přetečení, kompletnost, souvislost…),

b) kontrola vnitřního zpracování dat,

c) kontrola oprávněnosti běhu programů,

d) kontrola integrity dat,

e) kontrola obsahu generovaných dat.

Opatření musí zahrnovat i popis postupu při zjištění chyby.

Pokud UHN usoudí, že vytvářená aplikace by měla podporovat kryptografii, je nezbytné, aby byly podporovány mezinárodně uznávané standardy a dodrženy právní předpisy České republiky.

5.2 Data předávaná smluvním partnerům

Jedná se o chráněné informace předávané z UHN smluvnímu partnerovi na jakémkoliv nosiči, zejména jakékoliv listiny, interní dokumenty UHN, CD-ROM, diskety, pevné disky počítačů a jiné nebo zasílané e-mailem. Smluvní partner musí nakládat s předávanými daty dle tohoto dokumentu.

a) Předávání dat musí probíhat bezpečným způsobem.

b) Uchovávání a případné zpracování dat u smluvního partnera musí být prováděno tak, aby byla zajištěna jejich ochrana před neoprávněným přístupem a aby bylo znemožněno jejich zneužití.

c) Smluvní partner je povinen zajistit bezpečnou likvidaci již nepotřebných dat, případně médií s daty. Pro likvidaci medií nesoucích neveřejné informace musí být zvolena metoda, která zaručuje, že takto zlikvidované informace není možno běžně dostupnými prostředky obnovit (skartovačka, SW skartovačka).

Smluvní partner není oprávněn sám stahovat jakákoli data z IS UHN; vytváření souborů musí provést oprávněný zaměstnanec UHN a teprve takto vytvořená data smí být (na smluvním základě) předána partnerovi.

6 KB dodávek a služeb

6.1 Vývoj software smluvními partnery

1. Vývoj software musí probíhat:
    a. na testovacím prostředí odděleném od prostředí produkčního,
    b. na testovacích datech, která nejsou převzata z provozní databáze. Pokud je nutno použít data z provozní databáze, je nutno je anonymizovat,
    c. tak, že migrace do provozního prostředí může být provedena až po akceptaci výsledků testů ve vývojovém prostředí a formalizovaném a doložitelném odsouhlasení.
2. Přístup dodavatele do IS UHN

    Vzdálený přístup dodavatele může být povolen pouze za podmínek dohodnutých s vedoucím útvaru Informační a komunikační technologie nebo osobou, kterou pověří. O každém novém dodavateli, kterému se se zřizuje vzdálený přístup, bude informován manažer KB. Manažer KB má oprávnění vzdálené přístupy dodavatelů revidovat.

6.2 Dodávka software

1. U veškerého dodávaného programového vybavení musí být zřejmé, zda se jedná o volně šířený software nebo program podléhající licenční a registrační politice.