Bezpečnost citlivých údajů v geograficky rozlehlém systému OpenLIMS

M. Novotný

Tento text nastiňuje problematiku informační bezpečnosti laboratorního informačního systému OpenLIMS v souvislosti s fyzickým umístěním serverů. Měl by pomoci zodpovědět otázku, zda je z hlediska informační bezpečnosti zdravotnického zařízení provozujícího OpenLIMS (dále jen Provozovatel) vhodné dislokovat servery geograficky rozlehlého laboratorního systému za účelem poskytování komplexních servisních služeb do hostingového centra dodavatele systému.

1. VÝCHODISKA

Při zvažování variant bezpečnostní koncepce informačního systému je třeba vycházet z následujících otázek:

1) Co je předmětem ochrany a proč?
2) Jaké hrozí nebezpečí, od koho a jaký je motiv hrozby?
3) Jaká existují slabá místa systému umožňující případný bezpečnostní incident?
4) Jaký dopad může mít případný bezpečnostní incident?

1.1 Předmět ochrany

Neuvažujeme zde o úplné ochraně informačního systému OpenLIMS, ale omezujeme úvahy o bezpečnostní koncepci pouze na serverovou infrastrukturu, která sestává z fyzických prostor, v nichž jsou rozmístěny HW komponenty (servery, diskové pole, zálohovací systém, příslušné periferie), vlastních HW a SW komponent vč. výměnných datových nosičů a personálu oprávněného vstupovat do prostor serverového centra a popř. fyzicky manipulovat s výše zmíněnou technikou. Připustíme-li, že Provozovatel umístí serverovou infrastrukturu do prostor hostingového centra dodavatele, bude nucen uvažovat o ochraně v těchto bodech:

a) Laboratorní data uložená v LIS obsahují citlivé osobní údaje ve smyslu Zákona 101/2000 Sb. o ochraně osobních údajů. Proto je Provozovatel ze zákona povinen učinit veškerá opatření zabraňující jejich zneužití.
b) Provozovatel dále chrání údaje o svých klientech (zdravotnických zařízeních) a o provozu laboratoří jako své obchodní tajemství.
c) Záměrem Provozovatele je prezentovat svou obchodní činnost vůči klientům a případným akreditačním orgánům jako důvěryhodnou a splňující veškeré legislativní požadavky.

1.2 Bezpečnostní hrozby

Níže jsou vybrány některé druhy motivací a hrozeb, jež připadají v daném případě v úvahu:

a) Obecným (nenavázaným na konkrétní subjekt) motivem pro bezpečnostní incident může být pokus o zneužití citlivých osobních údajů. Hrozbou je zde útok na data ve smyslu odposlechu.
b) Motivem pro bezpečnostní incident v oblasti obchodní může být pokus ze strany konkurence poškodit dobrou pověst Provozovatele či dodavatele prokázáním skutečného nebo domnělého nesouladu provozu s legislativními požadavky na ochranu osobních údajů. Hrozbou je v tomto případě útok na data ve smyslu odposlechu a zveřejnění citlivých osobních údajů, jejich neoprávněná modifikace, poškození či zničení.
c) Obecným motivem může být krádež HW komponent. Hrozbou pro Provozovatele je primárně ztráta funkčnosti systému a sekundárně dobrého jména a obchodních příležitostí. Pro dodavatele jde o přímou ztrátu majetkovou a sekundárně o ztrátu důvěryhodnosti, neboť on ručí za hmotný majetek Provozovatele (popř. Provozovateli pronajímá svou techniku).
d) Další hrozby představují živelné katastrofy (povodeň, požár, elektrostatický výboj) a spontánní selhání techniky, jejichž následky pro Provozovatele mohou představovat širokou škálu dopadů od krátkodobé odstávky provozu až po úplnou likvidaci činnosti. Tyto hrozby však nepatří do kategorie záměrných útoků a existují nezávisle na dislokaci serverové infrastruktury.

1.3 Slabá místa serverové infrastruktury v prostředí laboratoří

Typickými slabinami v prostředí laboratoří jsou tyto:

a) Řízení přístupu osob do chráněných prostor serverového centra.
b) Smluvní podmínky s dodavatelem laboratorního informačního systému podchycující způsob ochrany dat, s nimiž dodavatel přichází při své činnosti do styku ať vzdáleně nebo lokálně.
c) Řízení přístupu k informacím v systému (zajištění principu autenticity uživatelů a nepopiratelnosti zodpovědnosti) konzistentně ve všech vrstvách systému a ve všech fázích životního cyklu předmětné informace.

d) Postup řešení havarijního stavu (Business Continuity Plannig) a obnova systému po havárii serverového centra (Disaster Recovery).

1.4 Dopady hrozeb

Dopady výše zmiňovaných hrozeb:

ad a) značně ohrožující obchodní činnost Provozovatele,

ad b) mohou mít likvidační důsledky,

ad c), d) citelná majetková ztráta a ohrožení obchodní činnosti.

Tyto dopady je třeba v rámci analýzy rizik konvertovat do měřitelné podoby s přihlédnutím k pravděpodobnosti reálného naplnění dané hrozby.

2. BEZPEČNOSTNÍ KONCEPCE

Musí umožnit eliminovat nebo snížit na únosnou míru výše naznačená rizika. Serverová infrastruktura je založena na technologii serverového klastru fy Microsoft (viz schéma níže) a je umístěna v hostingovém centru dodavatele systému OpenLIMS. Navrhovaná bezpečnostní koncepce disponuje těmito rysy:

- Ochrana dat před neoprávněným přístupem:
  Je realizována autentizačními mechanismy a přístupovými právy na úrovni operačního systému MS Windows 2003 Server, databázového systému MS SQL Server 2005 a vlastního aplikačního SW Stapro OpenLIMS.
- Řízení fyzického přístupu a chráněné prostory:
  Do chráněných prostor hostingového centra je přístup umožněn na základě biometrické autentizace, číselného kódu nebo pomocí mechanického klíče. V prvních dvou případech je o přístupu veden elektronický záznam a pohyb v chráněných prostorech zaznamenává kamera.
  Hostingové centrum disponuje požárními hlásiči, klimatizací a záložním napájecím zdrojem, za jejichž provoz zodpovídá pronajímatel na základě smluvního vztahu. Ten rovněž zodpovídá za řízení fyzického přístupu.
- Zajištění sledovatelnosti a auditu činností:
  Je zprostředkováno příslušnými funkcemi operačního systému, databázového systému a aplikačního SW. Auditní stopa může být plně pod kontrolou Provozovatele na základě výhradního využívání privilegovaného uživatelského účtu.
- Fail-Over Cluster serverů:
  Prakticky eliminují hrozbu spontánního selhání techniky a navíc umožňuje staticky rozložit výpočetní výkon např. dle území, na nichž se jednotlivé laboratoře nacházejí
- Systém zálohování dat:
  Lze jej koncipovat jako zálohovací automat s dvěma sadami vyjímatelných datových nosičů, z nichž jedna sada je uzavřena v trezoru mimo lokalitu hostingového centra a druhá je aktivně využívána. Data mohou být na nosič ukládána v zašifrovaném tvaru. Po určitém období (týden) se tyto sady vymění. Výměnu může provádět Provozovatelem určená osoba na základě smluvního vztahu. V případě poškození dat uložených na diskovém poli je možné tato obnovit ze zálohy a transakčního logu. V případě totálního zničení HW komponent včetně zálohovacího systému existuje sada datových nosičů v trezoru, takže nejdelší možná historie ztracených dat je dána periodou výměny sad.
- Servisní smlouva typu SLA:
  Smlouva uzavřená mezi Provozovatelem a dodavatelem podchycuje kromě parametrů a podmínek poskytované služby (zajištění provozu OpenLIMS) také závazky popř. sankce týkající se porušení informační bezpečnosti v případě řešení havarijního stavu.

3. DISKUSE K RIZIKŮM UMÍSTĚNÍ SERVEROVÉ INFRASTRUKTURY V HOSTINGOVÉM CENTRU

Z výše uvedeného vyplývají tyto skutečnosti:

1) Dodavatel systému má reálnou možnost data zneužít v rámci plnění svých smluvních povinností za účelem diskreditace Provozovatele nebo z nedbalosti. Tuto možnost však má bez ohledu na fyzické umístění serverů. Provozovatel je před tímto jednáním chráněn platnými trestně-právními předpisy. Je v zájmu dodavatele, aby k takovému incidentu nedošlo, protože je automaticky podezřelým ze spáchání trestného činu.
2) Osoba oprávněná manipulovat s výměnnými datovými nosiči nemá možnost data zneužít, protože jsou zašifrovaná. Tedy nezáleží na tom, zda jde o zaměstnance Provozovatele, dodavatele či jiné osoby.
3) Provozní prostředí HW komponent je zajištěno v rámci provozu hostingu. Toto je smluvně ošetřeno. Zde je možné zvažovat, zda provozní prostředí lépe zajistí dodavatel nebo Provozovatel.
4) Řešení havarijních stavů je zajištěno dodavatelem na základě SLA. V rámci toho existuje potenciální možnost zneužít data k poškození pověsti Provozovatele nebo z nedbalosti. To je však v přímém rozporu se zájmy dodavatele, který se zavázal k jejich ochraně v rámci SLA pod příslušnými sankcemi. Navíc by šlo o nezákonné jednání, které spadá do trestně-právní oblasti

a následně k poškození dobrého jména dodavatele. Tedy tato možnost se jeví jako nanejvýš nepravděpodobná.

4. ZÁVĚR

Podle našeho mínění neexistují důvody, které by z pohledu informační bezpečnosti jednoznačně bránily provozu serverové infrastruktury pro systém OpenLIMS mimo laboratorní zařízení Provozovatele za podmínky naplnění výše zmíněné bezpečnostní koncepce a dodržení celkové architektury řešení. Zda se stejné bezpečnostní úrovně dosáhne snáze a levněji provozem serverové infrastruktury v zařízeních Provozovatele nebo v hostingovém centru dodavatele, je otázka, na niž musí odpovědět analýza konkrétního případu.

Schema architektury rozlehlého laboratorního systému OpenLIMS