MEDAX Systems s.r.o.
Oběžná 2075/11, 709 00 Ostrava, Česká Republika
Tel.: +420 733 398 440
mail: podpora@medax.cz ,URL: www.medax.cz
Společnost vedená u Krajského soudu v Ostravě,
spisová značka C 30978

Zabezpečení osobních dat

Informační systém SmartMEDIX (dále Systém) vyžaduje určité podmínky pro běh z hlediska bezpečnosti dat a nabízí řadu možností, jak bezpečnost dat posílit.

Zajištění prostředí

Výchozím prostředím pro běh Systému je počítač nebo vnitřní síť počítačů s aktuálně podporovaným a aktualizovaným operačním systémem Windows společnosti Microsoft (nebo Linux pro databázový server). Komplementem operačního systému je zajištění zabezpečení systémové ochrany vhodným prostředkem, zjednodušeně antivirem s ochranou proti ransomware.

Systém pro svůj chod vyžaduje:

a) PC s vícejádrovým procesorem o taktu minimálně 2 GHz.
b) Operační paměť minimálně ~~4~~ 8 GB pro stanici a ~~8~~ 16 GB pro databázový server, lépe více.
c) Volný diskový prostor v řádu minimálně GigaBajtů na disku SSD.
d) Běžící databázový server Firebird nebo MS SQL Server v aktuálně podporované verzi;
e) Zabezpečený přístup k internetu (náležitě konfigurovaný a zaheslovaný router a další síťové prvky), náležité zabezpečení WI-FI sítě, je-li používána.
f) Záložní zdroj elektrické energie minimálně pro počítač s databázovým serverem optimálně pro všechny počítače přistupující k Systému.
g) Náležitě licencovaný a aktualizovaný operační systém a další SW komponenty.

Technická a organizační opatření

Základním opatřením je zabezpečení přístupu do prostor a k IT technice. Velmi důležitá je rovněž ochrana uživatelského účtu operačního systému Windows náležitým heslem. Vhodným opatřením je šifrování svazku či oddílu, na kterém Systém běží a jsou uchovávána data.

Aktualizace Systému

Systém má ve výchozím stavu nastavenou automatickou on-line aktualizaci při uvolnění nové verze. Průběžná aktualizace systému je nezbytná z hlediska vývoje zabezpečení a legislativy. V případě Nabyvatelem spravované aktualizace se lze přihlásit k odběru e-mailové informace o nové verzi.

Agenda přístupů

Systém nabízí řízení přístupu k datům v horizontální rovině řízením přístupu k položkám dokumentace a ve vertikální rovině řízení přístupu k jednotlivým záznamům.

Systém řeší zabezpečení dat těmito opatřeními:

a) Nutnost definice náležitě silného hesla pro přístup do Systému. Heslo musí být minimálně sedmiznakové, obsahovat velká i malá písmena a číslo nebo znak.
b) Základní rozdělení přístupu je rozšířený administrátorský přístup vs. uživatelský běžný přístup. Právo administrátor lze přiřadit jednotlivým uživatelům. Běžný uživatel nemá přístup do řady konfigurací vyhrazených pouze pro administrátora.
Upozornění: není-li administrátor nastaven, mají všichni uživatelé právo administrace (případ jednoho uživatele nebo velmi malé ambulance). V případě práce více uživatelů by měl být administrátor vždy nastaven.

MEDAX Systems s.r.o.
Oběžná 2075/11, 709 00 Ostrava, Česká Republika
Tel.: +420 733 398 440
mail: podpora@medax.cz ,URL: www.medax.cz
Společnost vedená u Krajského soudu v Ostravě,
spisová značka C 30978

c) Definice organizační struktury s hierarchií Zařízení [, Oddělení], Pracoviště, Personál. Uživatel se hlásí na příslušnou úroveň personálu a prováděné operace jsou zaznamenávány vzhledem k této úrovni.
d) Lze nastavit tato globální práva pro jednotlivé uživatele:
   - KONTAKT: právo vidět a použít pro výstup kontaktní údaje;
   - EXPORT: právo tisknout a exportovat;
   - STATUS: právo vidět stavové informace v zápatí aplikace.
e) Na úrovni personálu lze nastavit vertikální omezení přehledů. Omezení přístupu lze definovat např. na možnost vidět jen daným personálem pořízená data nebo vidět přehledová data jen přihlášeného pracoviště, oddělení, zařízení atp. Další možností omezení je nastavení počtu dnů zpět, po které může daný uživatel zobrazit data v přehledech (např. 7 dnů, 365 dnů apod.) separátně pro moduly ambulance, laboratoř, finance a pojišťovna.
f) Možnost nastavení horizontálních přístupových práv k položkám dokumentace prostřednictvím definice profilu práv a přiřazení daného profilu jednotlivému personálu. V praxi tak lze rozlišit role uživatelů v Systému, např. recepce, sestra, lékař apod.
g) Sdílení dokumentace umožňuje definovat dokumentační jednotky a přiřadit tyto jednotlivým pracovištím. Lze tak dosáhnout stavu, kdy pracoviště nebo skupina pracovišť odbornosti A pracuje a vidí svá data, které nevidí pracoviště ostatních odborností a naopak.
h) Soukromí/VIP je možnost skrýt data vybraných pacientů/klientů respektive řídit přístup k těmto datům pro jednotlivé uživatele. První uživatel-koordinátor, který si nastaví přístup k danému pacientovi/klientovi, se stává správcem a může přidávat oprávnění pro další uživatele.

Zálohování

Je nutno pravidelně zálohovat data na oddělený zabezpečený prostředek tak, aby bylo eliminováno riziko technického selhání, kybernetického útoku či odcizení počítače. Jako optimální se jeví každodenní zálohování.

Další opatření k posílení zabezpečení

Audit zabezpečení

Audit zabezpečení je nástroj analyzující nastavení Systému s identifikací rizikových či nedostatečně ošetřených míst.

Automatické uzamykání systému

Automatické uzamčení systému je vhodné řešit na úrovni systému Windows, aby nemohlo dojít k nežádoucí manipulaci s počítačem. Systém nabízí uzamykání, které lze nastavit v Konfigurace/Aplikace/Zabezpečení počtem minut, po kterém se při nečinnosti uzamkne.

Nezobrazení záznamů bez filtru v kartotéce

Výchozí zobrazení kartotéky je zobrazení pacientů s příjmením od A. Není úplně žádoucí, aby se záznamy pacientů z počátku kartotéky zobrazovaly po každém spuštění bez filtru. Systém nabízí nastavení *Nezobrazit záznamy pacientů, není-li zadán filtr (nezobrazit záznamy z počátku kartotéky)* v Konfigurace/Aplikace/Zabezpečení. Nadále zůstává, že si Systém ukládá posledně zvolený filtr kartotéky a při příštím zobrazení tento filtr použije (analogie záložky v knize).

MEDAX Systems s.r.o.
Oběžná 2075/11, 709 00 Ostrava, Česká Republika
Tel.: +420 733 398 440
mail: podpora@medax.cz ,URL: www.medax.cz
Společnost vedená u Krajského soudu v Ostravě,
spisová značka C 30978

Chráněná repozitoř

SmartMEDIX ukládá velká binární data (obrazová dokumentace, PDF) volitelně mimo hlavní databázi buď do zabezpečené složky nebo do separátní databáze. Z hlediska zabezpečení se jeví jako optimální řešení databázová repozitoř, ne souborové úložiště. Chráněnou repozitoř lze nastavit v Konfigurace/Aplikace/Obrazová dokumentace. Chráněnou repozitoř lze dále objektově zálohovat na cloud prostřednictvím volitelné nadstandardní služby.

Šifrování úložiště databáze

V rámci eliminace rizika zneužití dat při odcizení technicky je vhodným opatřením ochrana databáze i dalších souborů prostřednictvím šifrování. V systému Windows lze toto zabezpečení realizovat nástrojem BitLocker (ve verzi Professional či vyšší).

Nastavení náležitě silného administrátorského hesla pro přístup k databázi

Vždy je nutno nastavit dostatečně silné heslo pro administrátorský přístup a v žádném případě neponechávat výchozí heslo. Pokud na databázovém serveru běží i jiné systémy (zvací systémy, analyzátory, zobrazovací zařízení apod.), je nutno provést změnu hesla v součinnosti s dodavateli těchto systémů, aby nedošlo k omezení funkčnosti.

Při použití databáze Firebird je administrátorský účet SYSDBA.

Při použití databáze MsSQL Server je administrátorský účet dán buď autentifikací systému Windows, na kterém databáze běží, nebo administrátorským účtem (typicky sa, lépe alternativním) při ověřování samotným MsSQL serverem.

Nesdílení složky se souborem databáze

V žádném případě nelze sdílet složku se souborem databáze. Databázový server funguje jako služba systému a nevyžaduje sdílení složky se souborem databáze.

Ransomware

Specifickou hrozbou posledních let je ransomware. Ransomware je škodlivý program, který dokáže buď zašifrovat jednotlivé soubory nebo zamknout celý počítač. Za obnovení přístupů program požaduje zaplacení výkupného.

Nejčastěji se počítač infikuje ransomwarem, pokud spustíte zavirovanou přílohu e-mailu. Není výjimkou, že e-mailová zpráva pochází od někoho, koho znáte, a virus je skrytý ve zdánlivě neškodné příloze. Zpráva působí důvěryhodně až lákavě – chceme vám vrátit přeplatek, máme pro vás zásilku apod. Dalšími častými způsoby napadení ransomwarem jsou instalace neznámého programu nebo obecně spuštění podezřelého souboru. Nakazit se však lze i návštěvou webu, který tento typ malwaru obsahuje, nebo prostřednictvím počítačové sítě.

Ochrana proti ransomware

1) Pravidelné zálohování na oddělený zabezpečený prostředek;
2) Zabezpečené aktualizované prostředí viz úvod Zajištění prostředí;
3) Opatrnost – je nutno neotevírat odkazy a soubory z neznámých zdrojů;
4) Nastavení bezpečnostní politiky v organizaci a používání silných hesel;
5) Optimálně spolupráce se zkušeným partnerem na poli IT a kybernetické bezpečnosti.

MEDAX Systems s.r.o.
Oběžná 2075/11, 709 00 Ostrava, Česká Republika
Tel.: +420 733 398 440
mail: podpora@medax.cz ,URL: www.medax.cz
Společnost vedená u Krajského soudu v Ostravě,
spisová značka C 30978

Jedním z obecných doporučení je přesun IT prostředí do cloudu. Cloud nepochybně poskytuje vyšší míru zabezpečení než místní prostředí lékařské praxe nebo zdravotnického zařízení. V ČR však existuje případ, kdy po útoku ransomware padl celý cloud hostující data zdravotnických zařízení včetně záloh.

Velmi vysokou ochranu proti ransomware poskytuje nadstandardní služba replikace dat. Replikace představuje živou zálohu přenášející data mezi uzly s minimální latencí. V případě kolize jednoho uzlu je snadné tento uzel restaurovat daty z jiného funkčního uzlu. Pravděpodobnost, že by došlo k napadení všech uzlů současně, je velmi malá. Pro maximální eliminaci rizik je nutné zálohování i v případě replikace dat.

Informace Národního úřadu pro kybernetickou a informační bezpečnost:
https://nukib.cz/download/publikace/analyzy/Analyza_hrozby_ransomware.pdf

Závěr

Vzhledem ke komplexnosti problematiky zabezpečení chodu zdravotnické praxe z hlediska IT je důrazně doporučeno spolupracovat s profesionálním poskytovatelem služeb na tomto poli.

Ing. Marek Dobiáš

Digitálně podepsal Ing. Marek Dobiáš
Datum: 2024.11.20 10:37:26 +01'00'