FAKULTNÍ NEMOCNICE OLOMOUC

Úsek ředitele
Interní audit

AUDITORSKÁ ZPRÁVA
03/2015

Přístupová práva zaměstnanců do IS užívaných ve FNOL

Evidenční číslo IA	**03/2015**
Útvar, jehož činnost byla auditována	**Úsek informačních technologií**
Termín vykonání auditu	**od 10/2015 do 11/2015**
Auditované období	**01-09/2015**
Tým auditorů	**Mgr. Iveta Blahutová** **Mgr. Pavla Fiurášková**
Jména zpracovatelů AZ	**Mgr. Iveta Blahutová** **Mgr. Pavla Fiurášková**
Vypracování AZ	**24. 11. 2015 –08. 12. 2015**
Počet stran	**11**
Počet příloh	**0**
Počet vyhotovení	**3**

Rozdělovník	- **doc. MUDr. Roman Havlík, Ph.D., ředitel FNOL** - **ing. Jiří Marek, náměstek informačních technologií FNOL** - **Interní audit FNOL**

V Olomouci, listopad 2015

A) Úvod

Audit vykonaný na Úseku informačních technologií Fakultní nemocnice Olomouc (dále jen FNOL) byl proveden v souladu s ročním plánem interního auditu na rok 2015, schváleným ředitelem FNOL.

Cíl interního auditu:

- Prověřit, zda proces přidělování přístupových práv do IS ve FNOL probíhá v souladu s legislativou.
- Prověřit, zda zavedený systém přidělování přístupových práv k jednotlivým IS ve FNOL koresponduje s HR politikou FNOL.
- Prověřit, zda jsou data, uložená v IS ve FNOL zabezpečená proti zneužití.
- Prověřit, zda byla zavedena opatření související s možností zneužití dat v IS FNOL.
- Identifikovat možná rizika v souvislosti s přidělováním přístupových práv k IS novým i stávajícím zaměstnancům.
- V případě zjištění nedostatků doporučit opatření k nápravě.

Předmět interního auditu:

Identifikací, analýzou, hodnocením a dokumentací informací (Standard"2300 – Provedení auditu") shromáždit informace o všech záležitostech, jež souvisejí s cíly a rozsahem auditu tak, aby informace byly:

→ *dostatečné* = využitím nestatistického výběru vzorku i výběru vzorku pomocí standardních statistických metod,

→ *spolehlivé* = aby splňovaly požadavek § 7 odst. 1 zákona č. 563/1991 Sb., *o účetnictví,* v platném znění,

→ *užitečné* = zajišťovaly FNOL pomoc při plnění jejich cílů.

1) Legislativní rámec interního auditu:

Postup při výkonu auditu se obecně řídí zákonem č. 320/2001 Sb., *o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole)* v platném znění a Vyhláškou č. 416/2004 Sb., kterou se provádí zákon č. 320/2001 Sb., dále pak:

- Zákonem č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění,
- Zákonem č. 101/2000 Sb., Zákon o ochraně osobních údajů, v platném znění,

- Zákonem č. 432/2010 Sb., O kritériích pro určení prvku kritické infrastruktury, v platném znění,
- Nařízením vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury,
- Vyhláškou č. 317/2014 Sb., O významných informačních systémech a jejich určujících kritériích,
- Vyhláškou č. 316/2014 Sb., O bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti),
- Zákonem č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů,
- Pokynem č. CHJ – 2, k jednotnému uplatňování závazných pravidel a doporučení pro výkon interního auditu v orgánech veřejné správy,
- Pokynem č. CHJ – 9, pro výkon auditu shody v orgánech veřejné správy,
- Pokynem č. CHJ – 16, metodická pomůcka pro audit výkonu v orgánech veřejné správy.
- příp. další související legislativa.

2) Vnitřní normativní základna:

- Řád č. Řd-001 Organizační řád FNOL, 9. vydání ze dne 1. 5. 2013, 10. vydání účinné od 1. 7. 2014, v platném znění,
- Řád č. Řd-002 Pracovní řád, 4. vydání ze dne 23. 12. 2013, 5. vydání ze dne 8. 6. 2015, v platném znění,
- Sm-I001 Provozování informačních technologií a informačních systémů, 2. vydání ze dne 20. 5. 2010, 3. vydání ze dne 20. 4. 2015, v platném znění,
- MP-I001-01 Bezpečnost informačního systému a bezpečnost informací v informačních systémech, 2. vydání ze dne 20. 5. 2010, 3. vydání ze dne 20. 4. 2015, v platném znění,
- příp. další související vnitřní IŘA FNOL.

3) Pracovní postup:

- ❖ Termín provedení: 44. až 50. týden 2015
- ❖ Auditní metody: analýza a vyhodnocování
- ❖ Auditní postupy: revizní a hodnotící

- Druh auditu: audit výkonu, audit shody
- Útvar odpovědný za auditovanou činnost: Úsek informačních technologií
- Osoby odpovědné za auditovanou činnost: Náměstek informačních technologií
- Auditované období : období 01-09/2015.

B) Zjištění z vykonaného auditu

Audit se zaměřil na prověření procesu přidělování přístupových práv zaměstnancům do jednotlivých informačních systémů užívaných ve FNOL, odhalování rizik souvisejících s přístupem zaměstnanců do IS FNOL, specifikaci systémů, možnost řízení identit a v neposlední řadě na naplňování souladu mezi legislativou, vnitřními normami a praxí ve FNOL v oblasti IT. Zaměřil se na riziková místa v oblasti práce na PC a s tím související bezpečností a ochraně osobních údajů v IS FNOL.

V současné době informační systémy FNOL prochází přípravou na certifikaci dle normy ISO:27001. ISO 27001 je mezinárodní standard definující požadavky na systém managementu bezpečnosti informací. Systém managementu bezpečnosti informací je systematický přístup k řízení bezpečnosti důvěrných informací zahrnující zaměstnance, procesy, IT systém i strategii firmy. Obsahuje procesy definující přístup k vytváření, implementaci, provozu, monitorování, přezkoumání, udržování a zlepšování systému řízení informační bezpečnosti v organizaci.
Tato norma poskytuje komplexní přístup k informační bezpečnosti, pomáhá identifikovat, řídit a minimalizovat hrozby zneužití důvěrných informací. Aktiva, která je třeba chránit, zahrnují vše od informací v digitální podobě, přes papírové dokumenty a hmotný majetek (počítače a sítě), až po znalosti jednotlivých zaměstnanců.
Výhodou zavedení a certifikace systému bezpečnosti informací je soulad s legislativními požadavky (zákon č. 101/2000 Sb., O ochraně osobních údajů), nastavení systémového přístupu k ochraně informací, snížení rizik spojených s únikem informací z IS a jejich zneužitím, vyjasnění požadavků na záznamy v IS a dokumenty.

Zjištění I. :

Přístupová práva do IS jsou přidělena každému zaměstnanci při nástupu do FNOL. Každému nově příchozímu zaměstnanci je vygenerováno přístupové heslo do IS, které ho opravňuje k užívání určených IS. Přístup do jednotlivých určených IS užívaných ve FNOL je řízen potřebou přístupu do IS k výkonu práce jednotlivých konkrétních zaměstnanců, v jednotlivých IS lze poté rozlišovat přístupy zaměstnanců dle jednotlivých zaměstnaneckých kategorií (lékaři, nelékařští zdrav. pracovníci, THP).

Doporučovaná opatření I.:

Nejsou doporučována.

Zjištění II. :

Počet užívaných IS ve FNOL je poměrně vysoký, mnohé IS jsou specifické. Tyto IS jsou přístupné jen omezené skupině konkrétních zaměstnanců pracujících na určitých pracovištích (např. IS Lékárny, IS ÚČTO apod.). U těchto IS je nutný praktický výkon „garanta" jednotlivých aplikací, který po písemné žádosti vedoucího zaměstnance schválí přidělení přístupu zaměstnanci do konkrétní aplikace.

Doporučovaná opatření II.:

Dodržovat a prakticky plnit funkci „garanta aplikace" dle směrnice Sm-I001 u jednotlivých, specifických aplikací. Pozor na schvalování jednotlivých přístupových práv, nelze, aby si vedoucí pracovník sám schvaloval přístupová oprávnění do jednotlivých aplikací.

Termín: trvale **Odpovídá:** garanti aplikací

Zjištění III. :

Nově příchozím zaměstnancům je heslo vygenerováno, dostávají ho při úvodním zaměstnaneckém školení, stávající zaměstnanci (před zavedením této praxe) si své osobní heslo do IS FNOL zvolili sami. Zaměstnancům je doporučeno mít hesla složitá, kombinovaná z písmen a číslic, pracovníci IT doporučují hesla pravidelně měnit. V současné době však není žádný IS ve FNOL nastaven tak, aby byl zaměstnanec nucen po určité (předem nastavené době) heslo změnit, není aktivní nastavení exspirace hesla.

Problematika nastavení a utajení hesel souvisí s ochranou osobních údajů – v našem případě dat pacientů uložených v IS FNOL- a neoprávněným nahlížením do zdravotnické dokumentace. Tato problematika je opakovaně řešena v souvislosti vzájemného utajení – sdělování hesla do IS Medea mezi lékařskými a nelékařskými pracovníky na jednotlivých klinických pracovištích.

Přestože nelze vždy jednu fyzickou identitu spojit jen s jednou logickou (digitální) identitou, lze v IS FNOL vysledovat záznam každého zaměstnance v jednotlivých aplikacích.

Doporučovaná opatření III.:

Ze strany vedení FNOL přijmout takové opatření, podpořené IŘA, aby byly zaměstnanci automaticky jednotlivými aplikacemi „nuceni" k aktualizaci hesla. Pomocí vhodného motivačního nástroje (osobní údaje chráněné tímto heslem apod.) motivovat jednotlivé zaměstnance k vhodnému zacházení se svým heslem.

Při nastolení nové politiky povinné aktualizace hesel, trvat na dodržení nastavené politiky hesel (minimální, nepodkročitelné požadavky na tvorbu hesla – délka hesla, síla hesla, kombinace znaků, exspirace hesla, historie hesel).
Přestože nemá fyzická identita pouze jednu identitu logickou (digitální), zpětné vysledování pohybu zaměstnanců v jednotlivých aplikacích je možné.

Termín: 1. 3.2016 **Odpovídá:** náměstek UIT, vedení FNOL

Zjištění IV. :

Při odchodu zaměstnanců z FNOL jsou automaticky odebrány veškeré přístupy do IS, nejsou však mazány údaje z jednotlivých aplikací, vzniká tzv. spící identita.
Při odchodu zaměstnankyň na mateřskou, příp. rodičovskou dovolenou je zachován účet, který umožňuje pracovat s e-mailem.

Doporučovaná opatření IV.:

Nejsou doporučována.

Zjištění V. :

Přístupová práva pro zaměstnance „stážisty“ jsou aktivována na žádost vedoucího pracoviště a garanta probíhající stáže. Jsou vázána na konkrétní osobu a jsou časově omezena pouze na dobu stáže. Při ukončení doby stáže jsou automaticky přístupy odebrány, identita je dána do karantény a po jejím uplynutí je účet smazán (režim stejný jako u zaměstnance). Délka karantény je v tomto případě 1 rok.
Při dřívějším než plánovaném ukončení stáže je vedoucí pracoviště nebo garant stáže povinen tuto skutečnost nahlásit pomocí Help desk aplikace.
Přístupová práva pro studenty vyšších ročníků LF UP do NIS MEDEA jsou předmětem jednání. V současné době přístup studentům do NIS MEDEA není povolen, současný stav systému neumožňuje vydefinovat pro tuto skupinu uživatelů takovou úroveň vstupu.

Doporučovaná opatření V.:

Nejsou doporučována. Lze řídícím aktem aktualizovat povinnosti vyplývající vedoucím pracovišť a (nebo) garantům stáží v souvislosti s dřívějším ukončením stáže a odebráním přístupů do IS.

Termín: 1. 2.2016 **Odpovídá:** náměstek UIT, vedení FNOL

Zjištění VI. :

Při přihlašování IT zaměstnanců ve funkci „administrátor“ většina aplikací nepožaduje přihlašovací heslo IT zaměstnance a poté heslo „administrátora“, tzn., že umožňují pracovníkovi IT anonymní vstup do aplikace. Je-li IT pracovník přihlášen pouze jako „administrátor“, není možné označit konkrétního pracovníka, který jako „administrátor“ provedl v aplikaci změny.

Doporučovaná opatření VI.:

Při jakémkoli zásahu do aplikací ze strany pracovníků IT jako administrátorů je nutné, aby se přihlašovali svým loginem s administrátorskými právy a poté jako „administrátor“ z důvodu možnosti spárování konkrétního pracovníka s konkrétním zásahem do aplikací. Anonymní vstupy do aplikací omezit na nejnižší možnou míru, nejlépe zcela vyrušit.

Termín: trvale **Odpovídá:** náměstek UIT

Zjištění VII. :

Při změně fyzické identity zaměstnance, tzn. při změně pracovního zařazení, změně funkce, transferu na jiné pracoviště apod. jsou přístupová práva původního útvaru automaticky odebrána, a přidána výchozí pro nové pracoviště. Platí pro práva do počítačové sítě, přístup k některým aplikacím nezávisí na roli v PC síti (TreeInfo, MAJ, QI,...). K řízení uživatelských účtů je využívána aplikace Identity management (IdM). Aplikace je propojena s informačními systémy personálního odboru, odkud jsou data o nástupu zaměstnance, změně pracovního zařazení nebo odchodu zaměstnance čerpána. Nedochází k nabalování přístupových práv takovým způsobem, že nejsou odebrána práva vztahující se k výkonu předchozí funkce a jsou pouze přidána práva nová. Naopak nelze „dědit“ přístupová práva, tzn. automaticky povolit stejné přístupy.

Přístupová práva jsou zadávána ručně, což může nést procento chybovosti.

Doporučovaná opatření VII.:

Důsledně řídit uživatelská práva, nadále využívat a rozšiřovat aplikaci IdM.

Provádět kontrolu přístupových oprávnění a jejich rozsah v jednotlivých aplikacích dle pracovního zařazení a funkce zaměstnanců. Tyto kontroly provádět periodicky ve stanoveném období, na jednotlivých stanovených úsecích.

Pozor na neslučitelné role, schvalování přístupových práv jednotlivým vedoucím pracovníkům.

Termín: periodicky trvale **Odpovídá:** náměstek UIT

Zjištění VIII. :

Přístup k uložišti hesel je zabezpečen přístupovými právy na soubor hesel, soubor je zaheslován, heslo spravuje Oddělení správy systémů IT. Serverovna a uložiště citlivých údajů je zabezpečena dle standardních požadavků kladených na bezpečnost systémů, tzn., že je vybavena elektronickou zabezpečovací signalizací, kamerovým systémem se záznamem a každý přístup je monitorován.

V současné době není v IS FNOL stanovena a rozlišována citlivost obsažených dat v jednotlivých aplikacích.

Doporučovaná opatření VIII.:

Nejsou doporučována. V souvislosti s připravovanou certifikací ISO 27001, a možností, že na IS FNOL se bude vztahovat vyhláška č. 317/2014 Sb.,„o významných informačních systémech a jejich určujících kritériích“, a v rámci práce s riziky stanovit a rozlišit citlivost dat v IS FNOL a stanovit kritéria pro práci s nimi a přístup k nim.

Termín: k certifikaci **Odpovídá:** náměstek UIT

Zjištění IX. :

Bezpečnost a důvěrnost IS FNOL a informací v nich uložených není sledována.

Vyhodnocování bezpečnostních rizik neprobíhá. Ve FNOL není implementován globální nástroj na hodnocení bezpečnostních incidentů, je pouze sledována funkčnost jednotlivých aplikací.

Automaticky je chráněna aplikace Office Outlook užívaná na elektronickou komunikaci, denně je odfiltrováno až 80% spamových sdělení.

Ochrana rozhraní tiskáren a multifunkčních zařízení není v současné době žádná, problematika ochrany je řešena postupným připojováním těchto zařízení na samostatnou síť.

Doporučovaná opatření IX.:

Vydefinovat technické a kybernetické bezpečnostní incidenty, stanovit bezpečnostní rizika, zavést detekci bezpečnostních incidentů. Nastavit hodnocení aktiv.

Dořešit zabezpečit rozhraní tiskáren a multifunkčních zařízení.

Termín: 1. 3. 2016 **Odpovídá:** náměstek UIT

C) Závěr

Není pochyb o tom, že dnešní společnost je stále více závislá na používání a využívání informačních systémů. Tato závislost na informačních systémech a službách znamená, že organizace jsou zranitelnější ohrožením své bezpečnosti a bezpečnosti dat a informací, se kterými pracuje. Z tohoto důvodu je nutné, aby i FNOL přistoupila k bezpečnosti a důsledné ochraně užívaných informačních systémů.

V současné době probíhá na Úseku informačních systémů příprava k certifikaci systému managementu bezpečnosti informací dle normy ISO:27001. Systém managementu bezpečnosti informací v sobě zahrnuje management, politiku, organizaci i pravidelné přezkoumávání. Tato mezinárodní norma stanoví požadavky na systémy managementu bezpečnosti informací tak, aby byla organizace schopna vyhodnocovat svá rizika a uplatňovat náležité kontrolní a řídící mechanismy k zachování důvěrnosti, integrity a dostupnosti informací. Základním cílem je chránit informační aktiva, aby se informace nedostaly do nesprávných rukou nebo aby se neztratily navždy. Získání certifikátu certifikačním orgánem potvrzuje, že jsme přijali nezbytná opatření k ochraně citlivých informací před neoprávněným přístupem a změnami.
Příprava k certifikaci by měla být dokončena v co nejkratším termínu.
Splnění podmínek této normy a získání certifikátu pro FNOL znamená z velké části soulad s legislativou týkající se kybernetické bezpečnosti a znění zákona č. 181/2014 Sb., o kybernetické bezpečnosti a jeho prováděcích vyhlášek. Přestože informační systémy ve FNOL nespadají dle vyhlášky „o významných informačních systémech a jejich určujících kritériích“ mezi dotčené, je možné, či spíše reálné, že v blízké budoucnosti se zákon o kybernetické bezpečnosti bude informačních systémů a informací obsažených v IS FNOL bezprostředně dotýkat. Z tohoto důvodu a z důvodu citlivosti dat, se kterými IS FNOL pracují, je nutné tyto oblasti řešit s předstihem, včas se na tyto skutečnosti připravit a v neposlední řadě zavčasu alokovat potřebné finanční prostředky.

Ze závěru provedeného auditu vyplývá, že pro zachování a především zvýšení bezpečnosti a důvěrnosti IS FNOL bude vhodné v nejbližším období zavést management bezpečnostních informací a událostí SIEM. Tento bezpečnostní nástroj je schopný shromažďovat, analyzovat a prezentovat informace ze sítě a bezpečnostních zařízení, pomáhá spravovat identity a jednotlivé přístupy, identifikuje ohrožená místa. Tím že, shromažďuje a koreluje bezpečnostní i další informace v rámci celé síťové infrastruktury, včetně údajů z aplikací pro řízení identit a přístupů či dalších systémů, zařízení a aplikací, a pomáhá vyhodnotit shromážděné údaje,

identifikovat problémy s bezpečností a ověřuje jejich shodu s předpisy, se stává nenahraditelným nástrojem bezpečnostního managera.

V Olomouci dne 27. 11. 2015

Mgr. Pavla Fiurášková
Vedoucí interní auditorka

Mgr. Iveta Blahutová
Interní auditorka