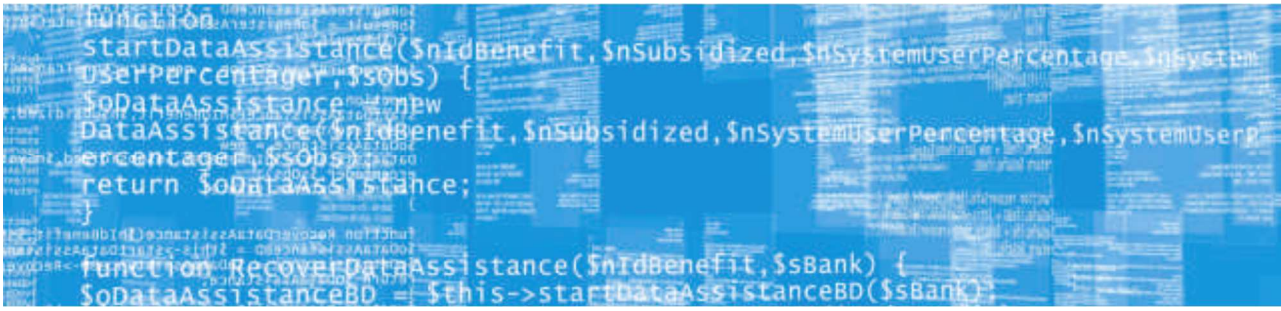
information and records management society
CZECH REPUBLIC GROUP



# Možná zranitelnost elektronických systémů spisové služby

*Stanislav Fiala*
*Martina Macek*
*Rudolf Vohnout*

*Praha, 10. srpna 2015*

# Obsah

# Možná zranitelnost elektronických systémů spisové služby

Spisová služba je páteřním procesem každého veřejnoprávního původce, v podstatě je páteřním procesem každé veřejnoprávní organizace. Pokud se jedná o určeného původce tedy veřejnoprávního původce, který má povinnost vykonávat spisovou službu v elektronické podobě v elektronických systémech spisové služby, je právě elektronický systém spisové služby jeho páteřním informačním systémem, který výše uvedený proces zabezpečuje.

Mezi určené původce patří ze zákona o archivnictví a spisové službě (zákon č. 499/2004 Sb.) organizační složky státu, ozbrojené síly, bezpečnostní sbory, státní příspěvkové organizace, vysoké školy, zdravotní pojišťovny, právnické osoby zřízené zákonem, kraje a hlavní město Praha.

V současné době však přibývá i původců, kteří nejsou určenými původci, a přesto zabezpečují proces spisové služby prostřednictvím elektronických systémů spisové služby a tyto systémy se stávají klíčovou komponentou jejich informačního systému i funkční architektury celé organizace.

Lze konstatovat, že v případě zastavení provozu tohoto informačního systému může dojít k fatálním následkům, a to k omezení nebo dokonce zastavení chodu úřadu, neboť chod každého úřadu je plně závislý na řádném průběhu všech procesů v celém životním cyklu dokumentů, bez kterých nemůže řádně vykonávat svoji činnost. Tyto procesy zahrnují příjem, označování a evidenci dokumentů, jejich rozdělování, oběh a vyřizování, vyhotovování a podepisování dokumentů, odesílání dokumentů jejich ukládání a vyřazování. Všechny tyto procesy jsou realizovány prostřednictvím elektronického systému spisové služby.

V našem příspěvku se však zaměříme pouze na možnou zranitelnost výše uvedeného systému u vstupně – výstupních procesů, kterými jsou příjem a odesílání dokumentů v digitální podobě přijímaných a vypravovaných prostřednictvím veřejné služby „e-mail“.

Příjem a vypravovaní dokumentů, ať již v podobě analogové nebo digitální, zabezpečuje u úřadu podatelna, přičemž příjem a vypravování dokumentů v digitální

podobě zabezpečuje její organizační součást, která pokrývá komunikaci jak prostřednictvím Informačního systému datových schránek, tak i prostřednictvím elektronické pošty.

Vyhláška o podrobnostech výkonu spisové služby č. 259/2012 Sb., přináší podrobný popis úkonů, které je nutné při přijmu dokumentů zabezpečit. Pro náš příspěvek je však nejdůležitější, že podatelna musí zpětně reagovat na jakýkoli doručený e-mail u kterého je uvedena elektronická adresa odesilatele v reálném tvaru. Tudíž musí odpovědět na e-mail, který splňuje, všechny formální požadavky přijmu, tak i na e-mail, který vykazuje určité vady, například obsahuje škodlivý kód.

## Důsledky připuštění nedůvěryhodného kanálu komunikace

Na elektronickou podatelnu přijímající dokumenty prostřednictvím veřejné služby „e-mail“ lze uskutečnit dva velmi jednoduché útoky, které její činnost paralyzuji, a to i za předpokladu, že systém i obsluha budou důsledně dodržovat výše uvedené povinnosti stanovené příslušnou legislativou.

**Útok č. 1** – Opakované robotické zasílání e-mailů, například s dotazem podle zákona o svobodném přístupu k informacím (zákon č. 106/1999 Sb.), zasílané z různých fiktivních adres, s obměňujícím se textem s logickým významem.

- z výše popsaných úkonů je zřejmé, že příjem dokumentů v digitální podobě je poměrně časově náročný proces, vzhledem k tomu, že takto generovaný e-mail splnil veškeré požadavky příjmu, musí jej obsluha elektronické podatelny zanést do systému elektronické spisové služby a předat k dalšímu zpracování. Odesílající stranu musí o příjmu vyrozumět, protože e-mail splnil všechny požadavky příjmu, a tudíž je známa adresa odesílající strany, byť fiktivní. K přetížení dojde jak na straně přijmu, zpracování, tak i odesílání.

**Útok č. 2** – Opakované robotické zasílání e-mailů zasílaných z různých fiktivních adres, s obměňujícím se textem, avšak s logickým významem. E-mail bude obsahovat škodlivý kód.

- po zjištění, že datová zpráva obsahuje škodlivý kód, musí být podatelnou zasílající strana, pokud je známa její adresa, o této skutečnosti vyrozuměna. K přetížení dojde jak na straně přijmu, zpracování, tak i odesílání.

V obou uvedených případech nelze na takto učiněná podání v první fázi nereagovat. Pokud je totiž při útoku generována formálně korektní konstrukce e-mailové adresy, nelze jednoznačně určit, zda se jedná o skutečnou adresu reálného odesilatele, nebo o fiktivně vygenerovanou adresu.

Slabina celého vstupně – výstupního procesu je v tom, že reakce musí nastat i na informace zaslané tak nedůvěryhodným zdrojem, jako je veřejný „e-mail“, a v první fázi musí podatelna reagovat i na e-maily, které neobsahují žádné autentizační prvky. Tudíž musí reagovat i na e-maily, které lze i automaticky generovat.

## Riziková integrace prostřednictvím webových služeb

Jiná možnost zranitelnosti vstupně – výstupního procesu vyplývá z toho, jak již bylo výše uvedeno, že elektronický systém spisové služby je „páteřním informačním systémem každého určeného původce“, takový páteřní informační systém je pak často integrován s dalšími informačními systémy, s kterými sdílí svá data. Dnes již je obvyklé, že elektronický systém spisové služby komunikuje s informačními systémy Datových schránek, Základními registry, CzechPointem, Registrem živnostenského podnikání a mnohými agendovými systémy.

Jednotlivé funkce elektronického systému spisové služby ovládají nejen jeho uživatelé, ale nepřímo i uživatelé napojených informačních systémů. Touto možností komunikace je vyzdvižen význam a přínos elektronického systému správy dokumentů, ale je tím zároveň zvýšena jeho zranitelnost. Komunikace integrovaných informačních systémů prostřednictvím elektronického systému spisové služby bývá často zabezpečována prostřednictvím webových služeb, takzvaných Web Services (WS). Útok přes WS je možný v zásadě třemi způsoby:

- generování velkého množství dotazů, které neprojdou autentizačním procesem, elektronický systém spisové služby je zařadí do fronty a vyřizuje tak, jak dojdou, s odpovědí „není oprávnění“,
- generování velkého množství požadavků s validní autentizací a maximem dotazů, které elektronický systém spisové služby zahltí,
- generování standardního množství požadavků s validní autentizací s nesmyslnými údaji, útočník se vloží do komunikace a svými požadavky záměrně mění standardní komunikaci, přičemž to netuší odesilatel původních požadavků ani jejich příjemce.

Výsledkem takovéhoto útoku může být zpomalený nebo nefunkční elektronický systém spisové služby, což může mít za následek nefunkčnost napojeného agendového informačního systému. Tímto může být například znemožněno včasné vyřízení žádosti o sociální dávky, které nebude možno následně včas vyplatit, a fatální kolapsy napojených systémů.

## ESSL jako významný informační systém

Elektronický systém spisové služby, jako jeden z klíčových informačních systémů organizace, dle definice zákona č. 181/2014 Sb. (Zákon o kybernetické bezpečnosti) spadá do kategorie tzv. významných informačních systémů[1]. Významné informační systémy jsou taxativně vyjmenovány v Příloze 1 vyhlášky 317/2014 Sb. Nad tento rámec jsou v Příloze 2 předmětné vyhlášky stanovena tzv. oblastní určující kritéria, na základě kterých lze stanovit, zdali daný systém spadá (či nikoliv) do definice významného informačního systému. Pro tento účel zpracovalo *Národní centrum kybernetické bezpečnosti* jako pomocný nástroj vývojový diagram[2] [2]. Z něho jednoznačně vyplývá, že systém spisové služby je v případě centrálních orgánů státní správy, krajských úřadů a celé řady dalších institucí veřejné správy významným informačním systémem. Dotčený subjekt veřejné správy je tak povinen dle zmíněného zákona provádět nejen relevantní bezpečností opatření, ale také zohlednit tyto požadavky při výběru významného informačního systému, resp. podpůrné informační infrastruktury.

Z praxe je však zřejmé, že dokud nedojde k bezpečnostnímu incidentu[3], jsou technická opatření prováděna pouze v rozsahu obecně definovaném v § 5 zákona o kybernetické bezpečnosti. Protože každý významný informační systém musí mj. obsahovat systém pro detekci, sběr a vyhodnocování kybernetických bezpečnostních událostí, lze v případě úspěšné detekce bezpečnostního incidentu v rámci nápravných

---

[1] Významným informačním systémem je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

[2] Proces určování podle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

[3] Kybernetický bezpečnostní incident je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.

opatření (§ 24 zákona) nařídit zákaz používání předmětného informačního systému, a to až do doby, než bude toto nebezpečí zažehnáno. V důsledku lze tedy, i v případě simulovaného útoku, docílit odstavení systému spisové služby a tím i ochromení chodu úřadu.

V tomto příspěvku nejsou uvažovány techniky jako sociální inženýrství, i když člověk v důsledku rozhoduje o závažnosti bezpečnostního incidentu a případném odstavení systému spisové služby. Útoky na infrastrukturu významného informačního systému tak lze rozdělit do dvou hlavních skupin:

- Útoky s cílem získání osobních či jiných citlivých údajů, včetně přístupových oprávnění – do této skupiny jsou zahrnuty útoky využívající známé bezpečnostní chyby, nerespektování doporučení či (závazných) pokynů při tvorbě hesla, či kompromitování přístupového certifikátu, například získání PIN kódu spolu s certifikátem (čipovou kartou).
- Útoky s cílem omezení či úplného vyřazení systému z provozu – tato skupina pokrývá útoky typu (d)DoS či další útoky na síťovou infrastrukturu (SYN FLOOD atd.), již zmíněné přehlcení legitimními požadavky nebo využití přítomnosti nástroje pro ochranu před škodlivým kódem a jeho zahlcení[4].

Útoky v druhé skupině jsou pravděpodobnější [1] a každý významný informační systém by měl být na tento typ útoku připraven. Útoky typu (d)DoS se odehrávají v menší míře pravidelně, avšak na cílený útok na konkrétní systém s použitím BotNetu musí být cíl připraven. Paradoxně obrana je jednoduchá, jak se ukázalo již v roce 2013, a tou je používání systému dDNS[5].

Dopadová kritéria dle vyhlášky 317/2014 Sb.[6] (Vyhláška o významných informačních systémech a jejich určujících kritériích), kdy nefunkčnost jednoho významného

[4] Každý požadavek přijatý systémem spisové služby musí před přijetím projít kontrolou přítomnosti škodlivého kódu (vir, malware apod.).

[5] Dynamic DNS. Principem je v relativně krátkých intervalech aktualizovat DNS záznamy, kdy doménové jméno (přiřazené významnému informačnímu systému) je překládáno na jinou IP adresu. Tj. systém spisové služby musí běžet na několika IP adresách (systémech) současně a dDNS mezi nimi provádí metodu „Round Robin“.

[6] O významných informačních systémech a jejich určující kritéria.

informačního systému může negativně ovlivnit funkčnost jiného informačního systému (v tomto případě by se jednalo například o tzv. IDM systém, tj. systém pro správu identit) jsou paralyzující v případě druhé skupiny, ale extrémně nebezpečná v případě první. Při snahách o tzv. SSO[7] napříč orgány veřejné správy, kompromitování přístupových údajů de facto znamená přístup do všech napojených informačních systémů.

Jako preventivní opatření proti útokům prováděným ze sítě internet se doporučuje integrace systémů IDS (nebo velmi měkce nakonfigurovaného systému IPS) do infrastruktury.

## Otázka na závěr

Závěrem našeho článku si musíme položit otázku, zda v některých případech elektronický systém spisové služby není systémem obsahujícím údaje o vice než 300 000 osobách. Pokud by tomu tak bylo, **jednalo by se o prvek kritické infrastruktury** (dle nařízení vlády 315/2014 Sb.) a nikoliv "pouze" o významný informační systém.

[1] fia, Novinky. *Útok na český internet pocházel z jednoho centra v Rusku* [online]. Praha, 2013. Naposledy aktualizováno 11. března 2013, 8:14. Dostupné z: http://www.novinky.cz/internet-a-pc/295624-utok-na-cesky-internet-pochazel-z-jednoho-centra-v-rusku.html

[2] Národní centrum kybernetické bezpečnosti: *Významné informační systémy* [online]. Verze 2.0. Praha, 2014. Dostupné jako PDF z: https://www.govcert.cz/download/nodeid-714/

[7] Single Sign On.

## Představení sdružení IRMS CRG

Information and Records Management Society – Czech Republic Group, z.s. je profesní organizací sdružující specialisty na problematiku správy informací a dokumentů (Information and Records Management) v České republice. **Sdružení je součástí mezinárodní asociace Information and Records Management Society** se sídlem v Londýně. Na základě příslušnosti k IRMS ve Velké Británii je sdružení oprávněno k udělování osobních certifikátů v oblasti správy dokumentů (Records Manager, ISO 15489 Lead Auditor) a k provádění auditu organizací podle normy ISO 15489.

Hlavním cílem spolku je podporovat a propagovat správné postupy správy a řízení dokumentů a informací a usilovat o zlepšování standardů kvality v oblasti jejich správy. Klíčovými činnostmi při naplňování tohoto globálního cíle jsou snaha o odborný růst a vzdělávání členů spolku, odborné i laické veřejnosti a podpora relevantního výzkumu a publicistiky.

Ve snaze o prosazení tohoto cíle uzavřel spolek **Memorandum o spolupráci s Ministerstvem vnitra České republiky** a na jeho základě je partnerem veřejné správy při přípravě certifikace a vzdělávání v oblasti správy dokumentů. V rámci své činnosti pak uzavřel další dílčí memoranda s významnými subjekty veřejné správy, jako je např. Ministerstvo financí, Ministerstvo spravedlnosti a další.

V rámci své činnosti připravil spolek IRMS **program akreditovaných vzdělávacích akcí**, jichž je obsahovým garantem a pro které certifikuje trenéry z řad svých členů. Jednotlivé kurzy jsou koncipovány tak, aby využívaly standardizovaných úrovní znalostí a skládaly se do uceleného vzdělávacího programu, který provádí specialisty v oblasti správy dokumentů v průběhu jejich kariérního růstu až na nejvyšší úrovně. Spolek rovněž pořádá **celou řadu dalších seminářů, školení a workshopů**, zaměřených na aktuální témata nebo na úzce vymezené problémy.

Klíčovou oblastí zájmu a aktivity spolku je problematika auditu správy dokumentů a spisové služby. V této oblasti vydal spolek **vlastní auditní metodický návod**.

## Členství v IRMS CRG

Spolek Information and Records Management Society je otevřen všem, kdo se zajímají o problematiku správy dokumentů a informací, ať už se jedná o organizace či jednotlivce.

Základní model členství v IRMS CRG je nastaven tak, aby vyhovoval jak potřebám odborných konsultantů a auditorů, kteří potřebují dostávat profesionální podporu a služby, tak široké odborné veřejnosti, která se v oblasti správy dokumentů a informací pohybuje a přeje si získat a rozvíjet vědomosti, případně získat vzdělání umožňující rozvíjení profesionální kariéry v této oblasti.

## Kontakty

**Sídlo a kanceláře sdružení se nacházejí na adrese:**

Thunovská 179/12
118 00 Praha 1

**Telefoní a mailová spojení**

Sekretariát: +420 222 559 569

Mail: info@irms.cz

URL: www.irms.cz

www.records-management.cz