Publikováno na *Ikaros* (https://ikaros.cz)

Digitálny repozitár ako terč kybernetického útoku

Anglicky

English title: Digital repository as a target of cyber attack
English abstract:
This paper points out selected general security issues of digital repositories and some known means of cyber attacks initiated against them within the global network. In the theoretical introduction, the authors rely on expert studies and articles drawn to the established topic. By means of the case study method in particular academic environment and their own experience gained in dealing with security incident in the digital library environment running the Invenio system, authors describe the important aspects of a critical migration of the system from one server to another. In this process, it is necessary to ensure the transfer of digital library objects and metadata related to them. At the end, the paper provides professional public incentives and motives for creating disaster recovery plan, in case their digital library does not have any yet.

Autoři: Formanek, Matúš [1]
Záborský, Martin [2]
Vydání: 2017, ročník 21, číslo 2 [3]
Rubrika: Výzkumná činnost [4]

Úvod

V posledných niekoľkých rokoch čoraz viac intenzívnejšie vníme zmenu úloh digitálnych knižníc a repozitárov – nastáva posun z prostého sprostredkovania prístupu k informáciám ku celej platforme sprístupňujúcej neustále sa rozširujúcu bázu znalostí rôznych komunít vo vnútri globálneho kontextu a s využitím moderných technológií (Chowdbury et al. 2006). Svoju úlohu však môžu digitálne knižnice dôsledne zabezpečovať len v prípade, ak dokážu svoje služby bezpečne a stabilne poskytovať aj prostredí „nebezpečného“ Internetu.

Joanne Kuzma (2010) skúmala túto problematiku vo svojom výskume, kde rozoberala bezpečnosť webových portálov vybraných 80 digitálnych knižníc v štyroch európskych krajinách. Pri pohľade do nedávnej minulosti poukazuje autorka napríklad aj na útoky hackerov na akademické digitálne knižnice v americkom štáte Indiana v rokoch 2002 a 2004. Kuzma (2010) týmto súčasne upozorňuje, že problematika bezpečnosti používateľských rozhraní digitálnych knižníc a repozitárov nie je ani dnes dostatočne preskúmaná. Navyše, odbornej komunite chýba dostatok literatúry k tejto téme.

Ďalší problém spočíva v tom, že samotní pracovníci knižníc si v širšom kontexte tohto problému častokrát neuvedomujú aspekty počítačovej bezpečnosti knižničných systémov a sietí, s ktorými pracujú (Fox 2006). Fox ďalej dodáva, že digitálny obsah môže byť v mnohých prípadoch veľmi cenný a pracovníci knižníc ho musia chrániť, tak ako chránia údaje o návštevníkoch. Uvedomujeme si, že títo pracovníci nie sú špecializovaní v oblasti IT systémov, no problematiku počítačovej bezpečnosti neslobodno podceniť a treba jej venovať náležitú pozornosť. Z podstaty tzv. Webu 2.0 vyplýva požiadavka správy používateľských identít a príslušných prístupových údajov používateľov webových aplikácií, ich telefónnych čísiel, adries, čísiel platobných kariet a podobne. Aplikácie Webu 2.0 sú spúšťané vo webových prehliadačoch, ktoré sú prostredníkmi medzi používateľmi a aplikáciami. Rôzne webové hrozby (tzv. exploity) majú dnes vyšší dopad, než kedykoľvek predtým (Šilić 2010).

Všetky webové aplikácie a systémy využívajúce pri svojej činnosti prostriedky siete, medzi ktoré radíme aj digitálne repozitáre, vyžadujú vhodne zvolený bezpečnostný mechanizmus, pretože uspokojujú informačné požiadavky mnohých používateľov. Zvýšená bezpečnosť je jedným z faktorov, ktoré môžu významne zvýšiť všeobecnú hodnotu týchto sieťových aplikácií a taktiež môžu prispievať k dosahovaniu vyššieho stupňa dôvery v prospech online služieb (Chen et al. 2006). Strata dôvery používateľov môže mať veľmi neblahé dôsledky, nehovoriac o riziku odcudzenia osobných informácií (Kuzma 2010).

Ako autori tohto príspevku si uvedomujeme dôležitosť prekladanej témy. Riešenie skutočného problému z praxe nám dodalo niektoré hodnotné skúsenosti, ktoré predkladáme zosumarizované formou prípadovej štúdie z konkrétneho prostredia.

Univerzitná dátová sieť

Vysoké školy a univerzity vo svete i na Slovensku sa neustále snažia držať krok s rýchlym vývojom v oblasti telekomunikačných služieb, ktoré ich spájajú s okolitým svetom. Vďaka častým inováciám dosahuje školská dátová

infraštruktúra pomerne vysokých kvalít, čo sa týka použitých technológií i rýchlosti prístupu ku globálnej počítačovej sieti Internet.

Na Slovensku zabezpečuje vo vzdelávacom sektore optické pripojenie k Internetu aj Slovenská akademická sieť SANET. Jedným z jej hlavných uzlov je aj Žilinská univerzita v Žiline (ďalej len ŽU), ako môžeme vidieť na mape nižšie.

[5]

Obrázok 1: Mapa uzlov siete SANET (zdroj: www.sanet.sk [6])

Z obrázka 1 je zrejmé, že v súčasnosti disponuje ŽU pripojením na úrovni až Nx100Gbit/s. Samozrejme, že konečná rýchlosť, ktorou sa pripájajú bežné študentské počítače v učebniach alebo lokálne mobilné zariadenia, je o niekoľko rádov nižšia, no vďaka svojmu rýchlemu uplinku, dokáže celá sieť uspokojiť bežné požiadavky veľkého množstva používateľov. Rýchlosť siete poskytuje, popri iných, pre univerzitu dôležitých systémoch, vhodné podmienky aj na prevádzku menších i väčších digitálnych knižníc a repozitárov.

Rýchla dátová infraštruktúra však môže paradoxne priniesť i niektoré problémy. Logicky sa dostávame k nasledovnému predpokladu: pokiaľ sa nejakému útočníkovi podarí získať určitý stupeň kontroly nad zariadením pripojeným rýchlou linkou (reálne rádovo do 1Gbit/s) k Internetu, dokáže priepustnosť siete významne zneužiť, či už na útoky typu DoS, rozposielanie spamu a pod. Potenciálne zraniteľné zariadenie s rýchlou linkou smerom von je pre útočníkov omnoho zaujímavejšie než podobné zariadenie s linkou o niekoľko rádov pomalšou, povedzme v domácom prostredí. Ako sme sa dozvedeli z viacerých zdrojov, s problémom kybernetických útokov dennodenne bojujú technickí pracovníci a administrátori snáď všetkých väčších organizácií, vrátane ŽU. Snažia sa odhaliť možné zraniteľnosti dátovej infraštruktúry ešte skôr, než ich objavia potenciálni kybernetickí útočníci. Ide však o veľmi náročnú úlohu. Terčom sa totiž môže stať teoreticky akýkoľvek server, či pracovná stanica, pretože nie je v možnostiach ich správcov vždy odhaliť všetky slabé miesta.

Druhy webových zraniteľností

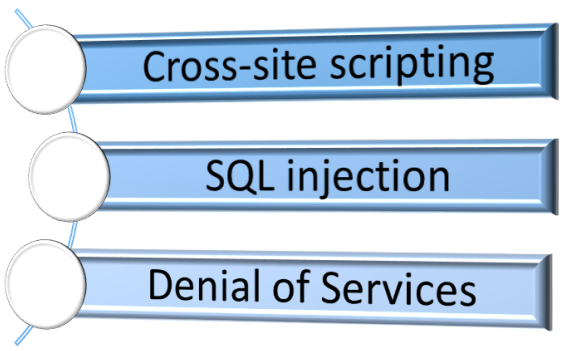
Komplexný systém digitálneho repozitára technicky pokrýva minimálne tieto súčasti:

- Základný operačný systém a potrebné služby na ňom spustené,
- databázu,
- webový server s príslušnými www stránkami, skriptami a pod.
- aplikačnú časť podporného softvéru knižnice

Každá z týchto súčastí otvára potenciálne zraniteľný priestor, v ktorom sa môže objaviť zraniteľnosť umožňujúca prienik do celého systému, resp. do jeho dôležitej časti.

V našom príspevku sa zameriavame predovšetkým na hrozby a bezpečnostné riziká webových rozhraní digitálnych knižníc. Potenciálne zraniteľné miesta vo webových prehliadačoch môžu útočníci využiť na vytvorenie škodlivých webových aplikácií kompromitujúcich bezpečnosť ich používateľov (Šilić 2012).

V odbornej literatúre nachádzame zvyčajne tri najčastejšie sa vyskytujúce hrozby, ktorými je možné (teoreticky) napadnúť akýkoľvek web. Jednotlivé druhy hrozieb sme na základe dostupných odborných článkov Katkara, Kulkarniho (2012) a Šilića (2010) rozdelili do troch skupín zobrazených na Obrázku 2.



[7]

Obrázok 2: Základné druhy hrozieb webových rozhraní

Uvedené druhy hrozieb nebudeme do detailov rozoberať, pretože ich dôkladný popis tvorí samostatnú problematiku presahujúcu rozsah jedného článku. Čitateľ si však môže podrobnosti nájsť v odbornej literatúre uvedenej v bibliografických odkazoch.

Len stručne spomeňme, že podstatou útoku typu *Cross-site scripting* (skrátene XSS) je zvyčajne zneužitie vstupov v skriptoch webových stránok, vďaka čomu môže útočník podstrčiť prehliadaču na vykonanie vlastný škodlivý kód. Zneužíva tak „dôveru“ používateľského prehliadača voči dátam prijímaným zo servera. (Šilić, 2012) Pomocou XSS dokáže útočník získať kontrolu nad systémom, čo mu následne umožní spúšťať vykonateľné príkazy, či zachytávať údaje u používateľoch a návštevníkoch webovej aplikácie.

Útok cez tzv. *SQL injection* prebieha vkladaním škodlivých príkazov do legitímnych SQL dotazov. Účelom je kompromitácia údajov lokálnej či vzdialenej SQL databázy, pretože útočníkovi z nej umožní získavať údaje. Tieto môže následne aj pozmeniť podľa ľubovôle.

Podstatou posledného menovaného útoku typu *Denial of Service* (skrátene DoS) je, ako už samotný názov napovedá, znefunkčnenie určitej služby či celého servera pre všetkých jeho používateľov spôsobom cieleného generovania obrovského, nadmerného objemu požiadaviek alebo iných dát, smerovaných na predmetný systém. Jeho systémové prostriedky sú zahltené a služba sa následne stáva nedostupnou.

Popis a priebeh reálneho kybernetického útoku

Predložená kapitola tvorí jadro celého príspevku. Formou prípadovej štúdie opisuje príklad z praxe, v ktorom došlo k zneužitiu akademického servera na nekalé účely. V závere opisujeme dôležité aspekty krízovej migrácie systému digitálneho repozitára z jedného servera na druhý.

V snahe o skvalitnenie procesov výučby mnohé vysoké školy a univerzity na Slovensku i vo svete radi experimentujú s nasadzovaním nových typov softvéru. S výhodou sa v mnohých prípadoch využíva v tomto smere open-source softvér kvôli určitému stupňu slobody, ktorá vyplýva z jeho podstaty. Pomocou príslušných nástrojov je možné týmto typom softvéru zabezpečiť prevádzku katedrovej či fakultnej digitálnej knižnice, prípadne aj celého elektronického repozitu.

V nasledovnej časti článku chceme poukázať na skutočnosti, ktoré sa objavili v praxi, priamo pri prevádzke menšieho testovacieho digitálneho repozitára slúžiaceho pre interné potreby Katedry mediamatiky a kultúrneho dedičstva pri FHV ŽU (ďalej len KMKD).

Opis pôvodného stavu

KMKD disponovala v novembri 2015 serverom s unixovým operačným systémom Ubuntu 12.04 vo verzii LTS (verzia systému s dlhšou dobou podpory) s pridelenou verejnou IP adresou a doménovým menom. Na tomto serveri bol nainštalovaný a spustený open-source softvér na podporu digitálnej knižnice Invenio vo verzii v1.0.0-rc0.578-5c51e, spoločne s databázou MySQL, ktorú využíval aj webový server Apache 2.2. Ten zabezpečoval funkčný rámec pre zobrazovanie webového rozhrania digitálnej knižnice a redakčného systému katedrovej webovej stránky. Internetová konektivita bola limitovaná rýchlosťou lokálnej sieťovej infraštruktúry na úrovni 100Mbit/s v smere download aj upload.

Priebeh útoku

Pomerne dlhý čas fungovali všetky služby spoločne na serveri bez akýchkoľvek problémov. Zlom nastal v momente, kedy boli IT administrátori univerzity upozornení na kontinuálne prebiehajúci DoS útok voči zahraničnému serveru. Z upozorňujúcej mailovej správy prijatej z dotknutej destinácie vyplynulo, že pôvodcom útoku je verejná IP adresa spomínaného katedrového servera. Došlo teda k jeho zneužitiu. Prvým krokom administrátorov bolo okamžité odstavenie infikovaného servera od Internetu, čo však spôsobilo nedostupnosť obsahu digitálnej knižnice, ako aj katedrovej webovej stránky.

Ďalším krokom bola analýza pôvodu útoku, spoločne s postupným obnovovaním nedostupných služieb. Správcovia IT zistili, že došlo k napadnutiu servera hackermi, pravdepodobne s využitím zraniteľnosti spusteného webového servera. Menovite išlo zrejme o útok typu Cross-site scripting. Lokálne administrátorské účty neboli podľa logovacích súborov kompromitované, no útočníkom sa podarilo získať na disku servera uložiť infikované php skripty, predovšetkým v dočasných priečinkoch (tzv. temporary folders) a adresároch spadajúcich pod webové stránky. Tieto poskytovali útočníkom potrebnú úroveň práv pre zápis a následné spustenie skriptu vykonávajúceho DoS útok smerom do zahraničia. Rýchlosť uploadu linky napadnutého servera teraz, paradoxne, spôsobovala ešte väčšie škody.

Obnovenie prevádzky

Kvôli náhlej nedostupnosti webovej stránky katedry, ako aj obsahu, ktorý digitálny repozitár poskytoval, bolo nutné okamžite adaptovať kroky vedúce k čo možno najrýchlejšiemu obnoveniu prevádzky oboch kritických služieb.

V bezpečných podmienkach bol opätovne spustený napadnutý katedrový server v núdzovom režime offline. Vykonala sa kontrola integrity príslušných databáz SQL, ktoré sa ukázali ako nedotknuté. Problémy sa však objavili pri kontrole webových stránok katedry a systémových súborov digitálnej knižnice Invenio. Moderný antivírusový systém zaznamenal veľké množstvo php súborov infikovaných vírusom PHP_WEBSHELL.VTJ, ktorý je podľa informácii

zverejnených na webovej lokalite Trendmicro.com, známy aj pod názvami PHP/SimpleShell a PHP/Agent.NDP. Časť výstupu z kontroly predmetných php súborov prikladáme nižšie ako Obrázok 3.

[8]

Obrázok 3: Časť zoznamu infikovaných súborov

Vďaka exploitu, ktorý v tomto prípade zaistil získanie vyššej úrovne prístupových práv (Dobšíček, Ballner 2004, s. 124), sa infikované súbory nachádzali sústredené výhradne v adresároch s právami na zápis pre webovú službu Apache, teda \opt\invenio\var\tmp\. Tieto adresáre sme rekurzívne zmazali, pretože neobsahovali žiadne údaje potrebné pre digitálnu knižnicu. Iná situácia však nastala v prípade katedrovej webovej stránky a jej súborov sústredených v adresári \var\www\. Webovú stránku katedry nebolo možné vôbec obnoviť do pôvodného stavu, pretože infikovaných bolo mnoho dôležitých súborov. Boli sme teda nútení siahnuť po staršej zálohe celého webu, ktorá sa vytvára periodicky. Na inom serveri sme spustili importovanú databázu redakčného systému a po zmene DNS záznamu spustili funkčnú verziu katedrovej stránky.

Presun objektov digitálnej knižnice a jej opätovné sprevádzkovanie bol proces omnoho náročnejší. Z bezpečnostných dôvodov sme sa rozhodli nenainštalovať digitálny repozitár Invenio na rovnaký server, na ktorom už bola spustená obnovená webová stránka. Použili sme dva samostatné servery – jeden pre webovú stránku katedry a druhý pre katedrovú digitálnu knižnicu Invenio.

Opätovnému spusteniu služieb digitálnej knižnice Invenio venujeme samostatnú kapitolu, pretože považujeme za nutné upozorniť sa niektoré nevyhnutné kroky spojené s migráciou systému na iný server.

Obnovenie prevádzky katedrovej digitálnej knižnice

Z pôvodného infikovaného servera sme skopírovali nedotknuté konfiguračné súbory Invenio, ako aj všetky digitálne objekty tejto knižnice, ktoré boli v našom prípade reprezentované najmä súbormi vo formáte PDF. K nim sa viažu patričné popisné či štrukturálne metadáta uložené v MySQL databáze. Vykonali sme tzv. dump lokálnej databázy, kontrolu jej konzistencie a premiestnili ju na nový server, kde sa nachádzala už čistá inštalácia novšej verzie softvéru Invenio, vrátane všetkých softvérových prerekvizít. Presunuli sme digitálne objekty knižnice i jej databázu, nastavili príslušné služby a server spustili. Neúspešne. Nový server digitálnej knižnice dostal pridelenú inú verejnú IP adresu, pretože jeho prevádzka je zabezpečená v inej serverovni, teda v rámci inej siete Univerzity.

Pôvodné konfiguračné súbory knižnice Invenio, vrátane odkazov v databáze obsahovali záznam o IP adrese ešte pôvodného katedrového servera, teda z času, kedy bola knižnica spustená paralelne spoločne s webovou stránkou katedry. Toto prvotné spojenie sa ukázalo spätne ako veľmi nevýhodné, nakoľko bolo nutné kompletne upraviť konfiguráciu novej knižnice s ohľadom na novopridelenú IPv4 adresu. Upravili sme konfiguračné súbory samotného softvéru Invenio a webového servera Apache 2.4 (pôvodne bola použitá verzia 2.2 využívajúca odlišné bezpečnostné politiky, čo migráciu ešte viac skomplikovalo).

Webový server nie je vo všeobecnosti problém spustiť pod inou IP adresou. Ak však ide o digitálny repozitár bez doménového mena, okamžite ako správcovia narazíme na problém s nefungujúcimi absolútnymi cestami jednotlivých elektronických dokumentov.

URL dokumentu, napríklad: http://158.193.111.222/niečo/subor.pdf [9] sa zmení na http://158.193.121.231/niečo/subor.pdf [10]. Zmena teda nastala v prípade migrácie našej knižnice na treťom a štvrtom oktete IPv4 adresy. Tieto zmeny je nutné uskutočniť aj v príslušných tabuľkách databázy MySQL. Pri tejto neľahkej úlohe nám veľmi pomohol skript, ktorý sme našli na internete: po zadaní konštánt CFG_URL_OLD (pôvodná stará IP adresa) a CFG_URL_NEW (nová IP adresa) sa skript pripojí k databáze a vykoná príslušné zmeny nad všetkými odpovedajúcimi tabuľkami. Myslíme si, že by tento skript mohol byť rovnako nápomocným všetkým používateľom

softvéru Invenio, a preto ho v úplnom pôvodnom znení, aj s menom autora, prikladáme v poslednej kapitole tohto článku.

Na záver migračného procesu digitálneho repozitára sme reindexovali celý obsah digitálnej knižnice a reštartovali weobú službu. Následne sa repozotár bez problémov spustil aj na novej IP adrese. V súčasnosti podnikáme kroky, ktoré umožnia prevádzkovať bezpečný protokol HTTPS miesto pôvodného HTTP.

Záver

Na príklade z praxe sme ukázali, že aj digitálne knižnice a repozitáre, rovnako ako iné systémy, sa môžu veľmi ľahko stať terčom kybernetických útokov. Navyše, tieto systémy môžu paradoxne figurovať i v neželanej pozícii pôvodcu incidentu.

Webové rozhrania všeobecne ponúkajú útočníkom častokrát hneď viacero spôsobov, ako preniknúť do celého systému. Úlohou pracovníkov knižníc je teda dbať na základy počítačovej bezpečnosti, úzko spolupracovať s odborníkmi v oblasti IT bezpečnosti, nechať si nimi starostlivo a pravidelne kontrolovať spustené služby a aktualizovať softvér, čím sa v konečnom dôsledku významne zníži riziko vzniku akýchkoľvek zraniteľností.

V každom prípade odporúčame, po porade s IT odborníkmi, vypracovať odpovedajúci *disaster recovery* plán, pretože náhla migrácia počítačových údajov či celých systémov, prípadne zmena konfigurácie, môžu spôsobiť nepripraveným správcom značné problémy, prípadne aj stratu cenných údajov, o strate používateľskej dôvery nehovoriac.

Skript

Autorom skriptu uvedeného pod čiarou je Tibor Šimko (2011). Telo skriptu stačí umiestniť do textového súboru, upraviť konštanty v úvode, prideliť súboru práva na vykonávanie a následne ho spustiť v niektorom z unixových operačných systémov.

```
#!/usr/bin/env python

"""Small script to update URLs in bibfmt's XM values in situ. Use with care!"""

CFG_URL_OLD = 'http://somebox.foo.com/'

CFG_URL_NEW = 'http://bar.org/'

import sys

import zlib

from invenio.dbquery import run_sql

from invenio.search_engine import search_pattern

recids = search_pattern(p=CFG_URL_OLD + '*', f='8564_u', m='e')

nb_all = len(recids)

nb_done = 0

print '[INFO] Will process %d records...' % nb_all

for recid in recids:

    try:

        nb_done += 1

        marcxml = zlib.decompress(run_sql("SELECT value FROM bibfmt WHERE format='xm' AND id_bibrec=%s", (recid,))[0]
[0])

        marcxml = marcxml.replace(CFG_URL_OLD, CFG_URL_NEW)

        run_sql("UPDATE bibfmt SET value=%s WHERE format='xm' AND id_bibrec=%s", (zlib.compress(marcxml), recid))

        run_sql("DELETE FROM bibfmt WHERE format='recstruct' AND id_bibrec=%s", (recid,))

        print '[INFO] %d/%d, record %s, XM format successfully updated.' % (nb_done, nb_all, recid,)

    except:

        print '[ERROR] %d/%d, record %s, XM format update led to errors!' % (nb_done, nb_all, recid,)

    sys.stdout.flush()

print '[DONE]'
```

Literatura:

- Dobšíček, M., Ballner, R. 2004. *Linux : bezpečnost a exploity.* České Budějovice : Kopp. ISBN 80-723-22-435

- Fox, E., ElSherbiny N. 2011. Security and Digital Libraries [online]. In: *InTech open*. [cit. 2017-02-20]. DOI: 10.5772/15762
- Fox, R. 2006. Digital Libraries: The Systems Analysis Perspective, Vandals at the Gates. In: *OCLC Systems & Services : International digital library perspectives*. Vol 22, Iss 4, p.249-255. ISSN: 1065-075X
- Chen, S., Choo, C., Chow, R. 2006. Internet Security: A Novel Role/Object-Based Access Control for Digital Libraries. In: *Journal of Organizational Computing and Electronic Commerce,* vol.16, Iss 2, p. 87-103.
- Chowdhury, G., Poulter, A., McMenemy, D. 2006. Public Library 2.0: Towards a new mission for public libraries as a ‘network of community knowledge. In: *Online Information Review*, vol30, Iss 4, p. 454-460. ISSN: 1468-4527
- Katkar, S., Kulkarni, B. 2012. Web Vulnerability Detection and Security Mechanism [online]. In: *International Journal of Soft Computing and Engineering (IJSCE)*. [cit. 2017-02-10]. Vol 2, Iss 4. ISSN: 2231-2307. Dostupné z: https://pdfs.semanticscholar.org/fbd4/f516b9e6b7b0fc266be421e63a01dd438921.pdf [11]
- Kuzma, J. 2010. European Digital Libraries: Web Security Vulnerabilities [online]. In: *Library Hi Tech.* Vol 28, Iss 3, p. 402 – 413. [cit. 2017-01-29]. ISSN: 0737-8831. DOI: http://dx.doi.org/10.1108/07378831011076657 [12] Dostupné z: https://eprints.worc.ac.uk/975/1/librariessecunov09revised1.pdf [13]
- Simko, T. 2011. *How To Change Site URL* [online]. [cit. 2017-01-05]. Dostupné z: https://github.com/tiborsimko/invenio-devscripts [14]
- Šilić, M. 2010. *Security Vulnerabilities in Modern Web Browser Architecture* [online]. [cit. 2017-03-01]. Dostupné z: https://www.researchgate.net/publication/224163004_Security_vulnerabilities_in_modern_web_browser_architecture [15]

Hodnocení:

Průměr: 5 (hlasů: 7)

URL zdroje: https://ikaros.cz/node/17971

Odkazy

[1] https://ikaros.cz/autor/formanek-matus
[2] https://ikaros.cz/autor/zaborsky-martin
[3] https://ikaros.cz/vydani/2017-rocnik-21-cislo-2
[4] https://ikaros.cz/rubrika/aktualni-rubriky-a-sloupky/vyzkumna-cinnost
[5] https://ikaros.cz/images/201702/formanek1.png
[6] http://www.sanet.sk/
[7] https://ikaros.cz/images/201702/formanek2.png
[8] https://ikaros.cz/images/201702/formanek3.png
[9] http://158.193.ABC.DEF/niečo/subor.pdf
[10] http://158.193.GHI.JKL/niečo/subor.pdf
[11] https://pdfs.semanticscholar.org/fbd4/f516b9e6b7b0fc266be421e63a01dd438921.pdf
[12] http://dx.doi.org/10.1108/07378831011076657
[13] https://eprints.worc.ac.uk/975/1/librariessecunov09revised1.pdf
[14] https://github.com/tiborsimko/invenio-devscripts
[15] https://www.researchgate.net/publication/224163004_Security_vulnerabilities_in_modern_web_browser_architecture