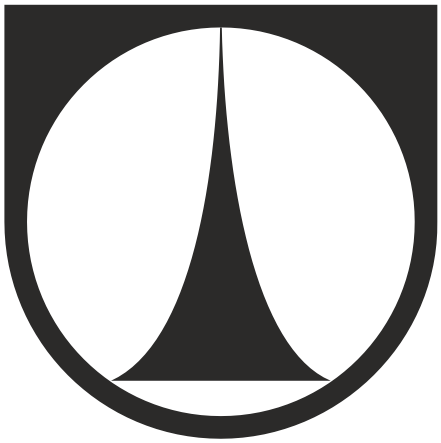
TECHNICKÁ UNIVERZITA V LIBERCI
Ekonomická fakulta



DIPLOMOVÁ PRÁCE

2013 **Bc. Vojtěch Kočí**

TECHNICKÁ UNIVERZITA V LIBERCI
Ekonomická fakulta

Studijní program: **N 6209 – Systémové inženýrství a informatika**
Studijní obor: **Manažerská informatika**

Autorizace webového obsahu

Authorization of web content

DP – EF – KIN-2013-08
Vojtěch Kočí

Vedoucí práce: doc. Ing. Jan Skrbek, Dr., katedra informatiky
Konzultant: Ing. Zbyněk Hubínka, katedra informatiky

Počet stran: 64 Počet příloh: 0

Datum odevzdání: 20. 12. 2013

TECHNICKÁ UNIVERZITA V LIBERCI
Ekonomická fakulta
Akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	Bc. Vojtěch Kočí
Osobní číslo:	E11000084
Studijní program:	N6209 Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Název tématu:	Autorizace webových obsahů
Zadávající katedra:	Katedra informatiky

Zásady pro vypracování:

1. Současný stav a trendy rozvoje Internetu z hlediska sdílení webových obsahů
2. Identifikace a analýza rizik
3. Návrh možností eliminace rizik
4. Zhodnocení navržených řešení

Rozsah grafických prací:

Rozsah pracovní zprávy: **65 normostran**

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

STŘIHAVKA, M. Vaše bezpečnost a anonymita na Internetu. 1. vyd. Praha: Computer Press, 2001. ISBN 80-7226-586-5.
ČERMÁK, J. Internet a autorské právo. 2. vyd. Praha: Linde, 2003. ISBN 80-7201-423-4.
JAKOBSSON, M. The dead of the Internet. 1st ed. New Jersey: John Wiley & Sons, 2012. ISBN 978-1-118-06241-8.
Elektronická databáze článků ProQuest (knihovna.tul.cz).

Vedoucí diplomové práce: **doc. Ing. Jan Skrbek, Dr.**
Katedra informatiky

Konzultant diplomové práce: **Ing. Zbyněk Hubínka**
Katedra informatiky

Datum zadání diplomové práce: **30. října 2013**

Termín odevzdání diplomové práce: **7. května 2014**

doc. Ing. Miroslav Žižka, Ph.D.
děkan

Technická univerzita v Liberci
Ekonomická fakulta
L.S.

doc. Ing. Jan Skrbek, Dr.
vedoucí katedry

V Liberci dne 30. října 2013

Prohlášení

Byl jsem seznámen s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé diplomové práce pro vnitřní potřebu TUL.

Užiji-li diplomovou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Diplomovou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím diplomové práce a konzultantem.

V Liberci dne 5. prosince 2013 Bc. Vojtěch Kočí

Poděkování

Na tomto místě bych rád poděkoval vedoucímu mé práce panu doc. Ing. Janu Skrbkovi, Dr. za trpělivost a cenné rady. Dále bych rád poděkoval svému nejbližšímu okolí a rodině za podporu při psaní této práce.

Anotace

Tato diplomová práce je zaměřena na autorizaci webového obsahu, resp. autorizaci uživatelů do webových aplikací. Protože je na internetu možné provozovat trestnou činnost, jsou zde rozebrány i legální aspekty spojené s internetem a internetovou komunikací. V teoretické části je rozebrán vývoj internetu ve světě a zvlášť v České republice se zaměřením zejména na síť CESNET. V praktické části je pak vysvětleno, proč je důležité autorizovat webový obsah, dále je zde několik příkladů typických útoků (phishing, pharming) spojených se špatnou autorizací na internetu. V poslední části praktické části se diplomová práce zabývá jednotlivými možnostmi autorizace na webových aplikacích, kde jsou analyzovány jejich rizika a navrhnuta možná řešení těchto rizik.

Klíčová slova

Bezpečnost na internetu, DNS cache poisoning, DNSSEC, DNS spoofing, Phishing, Pharming, SSL/TLS, Šifrování s veřejným klíčem

Annotation

This thesis is focused on authorization of web content, respectively user authorization to web applications. Because crimes can be committed on the internet, the legal aspects associated with internet and internet communications are discussed as well. The development of the internet in the world and in the Czech Republic with focus on CESNET network is analyzed in the theoretical part. The importance of web content authorization is explained in the practical part. There are also some examples of typical attacks (phishing, pharming) associated with a bad authorization on the internet. Last part of practical part deals with user authorization to web applications, where the risks are analyzed and proposed solutions to these risks.

Key Words

DNS cache poisoning, DNSSEC, DNS spoofing, Internet security, Phishing, Pharming, Public key encryption, SSL/TLS

Obsah

Seznam zkratek

TUL	*Technická univerzita v Liberci*
ARPA	*Advanced Research Projects Agency*
NCP	*Network Control Protocol*
TCP	*Transmission Control Protocol*
IP	*Internet Protocol*
NSF	*Nacional Science Foundation*
EARN	*European Academic Research Network*
FESNET	*Federal Education and Scientific NETwork*
CESNET	*Czech Scientific and Education NETwork*
SANET	*Slovenská Akademická a datová síť*
EU	*Evropská unie*
CEF	*Customer Empowered Fibre Network*
DWDM	*Dense Wavelength Division Multiplexin*
IPTV	*Televize přes internet*
VoIP	*Telefonie přes internet*
Wi-Fi	*Wireless Fidelity*
CMS	*Content Management Systém*
PHP	*Personal Home Page*
MVC	*Model View Controller*
IPsec	*Internet Protocol Security*
SSL	*Secure Socket Layer*
TLS	*Transport Layer Security*
CA	*Certifikační Autorita*
VPN	*Virtual Private Network*

Seznam tabulek

Seznam obrázků

Úvod

Tato diplomová práce bude zaměřena na autorizaci webového obsahu resp. autorizaci uživatelů do webových aplikací. Protože jsou webové aplikace spojeny s internetem, budou zde odhadnuty budoucí trendy internetu vzhledem k jeho vývoji v minulosti. Cílem této diplomové práce je zjistit způsob, jakým by bylo možné zajistit bezpečné procházení internetu pro jakéhokoli uživatele a jejich bezpečnou autorizaci do webových aplikací.

V dnešní době existuje hodně hrozeb na internetu, díky kterým může uživatel internetu nevědomě předat citlivé údaje (osobní, firemní) třetí osobě, která je může zneužít ve svůj vlastní prospěch, případně může útočník uživatele přesměrovat na nebezpečné stránky a vystavit ho trestnímu stíhání. Právě z těchto důvodů je nutné se zaměřit na autorizaci webového obsahu, aby byl internet bezpečný pro všechny uživatele. Tato práce bude rozdělena do dvou částí, první část se skládá z literární rešerše a teoretické části, druhá část je praktická část, kde budou prozkoumány jednotlivé možnosti autorizace webového obsahu a autorizace uživatelů do webových aplikací včetně identifikování rizik.

V teoretické části práce je charakterizován vývoj internetu ve světě i v České republice, se zaměřením zejména na síť CESNET, která byla největší sítí v České republice a určovala tak rozvoj internetu. Protože se v této práci jedná o autorizaci webového obsahu, je teoretická část věnována částečně i tvorbě webových stránek. Dále zde bude charakterizováno právo na internetu (včetně příkladů z praxe), definování pojmů jako ISP, definiční autorita apod., nebude opomenuto ani právo na internetu a mezinárodní spolupráce, protože díky faktu, že je internet celosvětový, toto téma nelze opomenout. V poslední řadě bude poukázáno na vývoj práva souvisejícího s datovými komunikacemi v České republice.

V praktické části je vysvětleno, proč je důležité autorizovat webový obsah a dále možnosti, jak toho dosáhnout globálně pomocí implementace bezpečnostního rozšíření DNSSEC na servery DNS, tak i autorizací uživatelů do webových aplikací. Autorizace uživatelů do webových aplikací bude provedena čtyřmi způsoby a u všech budou identifikována rizika. V této části dále budou také rozebrány jisté hrozby špatné autorizace, např. přesměrování

uživatelů a možné obrany proti těmto druhům útoků. Poslední částí bude zhodnocení jednotlivých druhů autorizace a jejich bezpečnost.

Literární rešerše

Obecně platí, že zabezpečení webových služeb je široká a složitá oblast zahrnující řadu technologií. V současnosti je velké úsilí o poskytování bezpečných služeb např. autentifikace mezi zúčastněnými subjekty, utajení a integrity komunikace. K tomu může přispět několik existujících technologií: TLS/SSL (Rescorla, 2001) a IPsec (Kent & Atkinson, 1998). Také existuje zabezpečení založené na XML podpisu (Barel et al., 2001).[1]

V současné době není žádná specifikace ani standard pro autorizování webových služeb. Nyní většina aplikací založených na webových službách prochází procesem autentifikace, poté následuje proces autorizace, který využívá funkci specifickou pro každou aplikaci, která určuje přístup pro každého uživatele (často se vymýšlí ty samé věci dokola).[1]

Málo technologií je více kritických pro fungování internetu než DNS, a DNSSEC poskytuje způsob, jak zajistit, že online spojení je se správnými webovými stránkami nebo službami. [2]

DNS bylo navrženo tak, že bezpečnost nebyla hlavní oblastí zájmu. Bylo identifikováno několik druhů útoků.[3] Útočník těchto slabin může využít, aby podstrčil falešné DNS data k přesměrování uživatelského provozu (například prohlížení webu webů)

---

[1] INDRAKANTI, S., VARADHARAJAN, V. and HITCHENS, M. Authorization Service for Web Services and its Application in a Health Care Domain. *International Journal of Web Services Research*, Oct, 2005, vol. 2, no. 4. pp. 94-119 ProQuest Central; ProQuest Technology Collection. ISSN 15457362.

[2] INTERNET SOCIETY, Internet Society Collaborates with Shinkuro and Parsons to Promote Global Deployment of Domain Name System Security Extensions DNSSEC. *Bioterrorism Week*, červenec 29, 2013. pp. 10 ProQuest Central; ProQuest Hospital Collection; ProQuest Natural Science Collection. ISSN 15478602.

[3] BELLOVIN S., "Using the DNS for System Break-Ins," Proc. Usenix, Security Symp., 1995

na podvodné a často nebezpečné stránky, což vede k odepření služby nebo k narušení bezpečnosti.[1]

DNSSEC má potenciál na zesílení internetové infrastruktury pomocí ověřování původu DNS dat a ověření jejich integrity při pohybu přes internet. DNSSEC chrání internetovou komunitu před zapomenutými DNS daty, pomocí kryptografie s veřejným klíčem, která digitálně podepisuje DNS data. Digitální podpis dokáže zaručit, že s daty v průběhu přenosu nebylo nikterak manipulováno a pocházejí z požadovaného zdroje. DNSSEC může také dokázat, že doménové jména neexistují. Výsledkem je, že DNS dotazy a odpovědi jsou chráněny před paděláním, které by mohly přesměrovat uživatele internetu na phishingové stránky a pharmingové stránky, nebo útoky typu „men in the middle", které zachytávají komunikaci mezi dvěma systémy.[2]

DNSSEC je důležitou součástí počítačové bezpečnosti, ale není bezchybné a naprosto bezpečné řešení. DNSSEC neřeší mnoho nejčastějších hrozeb pro bezpečnost na internetu. Proto jsou další vrstvy ochrany jako „Rozšířená validace SSL certifikátů a dvou-faktorová autentifikace" nezbytné k zabezpečení internetu pro všechny.[1]

DNSSEC zabraňuje hackerům před přesměrováním provozu na síti a nasměrováním ho na své podvodné stránky. Internetový standard zabraňuje útokům na DNS (DNS spoofing) povolením ověření doménového jména vůči odpovídající IP adrese použitím digitálního podpisu a šifrování s veřejným klíčem.[3]

---

[1] YANG, H., et al. Deploying Cryptography in Internet-Scale Systems: A Case Study on DNSSEC. *IEEE Transactions on Dependable and Secure Computing*, Sep, 2011, vol. 8, no. 5. pp. 656-669 ProQuest Central; ProQuest Technology Collection. ISSN 15455971. DOI http://dx.doi.org/10.1109/TDSC.2010.10.

[2] *VeriSign Announces DNSSEC Deployment Support Plans to Enhance Internet Security.* Miami: listopad 16, 2009 ProQuest Central.

[3] MARSAN, C.D. Domain Vendors Tackle DNS Security. *Network World*, Dec 15, 2008, vol. 25, no. 48. pp. 10 ProQuest Central; ProQuest Technology Collection. ISSN 08877661.

DNSSEC je považován za nejlepší cestu k posílení DNS proti jeho slabinám jako Kaminskeho bug, který byl objeven v létě 2008. Právě kvůli těmto hrozbám se rozhodla americká vláda k nasazení DNSSEC na domény .gov a .mil.[1]

Z kryptografického pohledu se DNSSEC zaměřuje spíše na mírné cíle, design by měl být jednoduchý a nasazení by také nemělo být složité. Nicméně realita je jiná. Snaha vyvinout DNSSEC začala v polovině devadesátých let, a trvalo to několik let a tři kola revizí, aby byla specifikace dokončena v březnu 2005[2,3,4].

Architektura zabezpečení internetového protokolu (IPsec) se skládá ze souboru protokolů[5,6,7] vyvinutých pro zajištění integrity bezpečnostní služby, důvěrnosti a autentifikace datové komunikace přes IP síť[8,1].

---

1 MARSAN, C.D. Domain Vendors Tackle DNS Security. *Network World*, Dec 15, 2008, vol. 25, no. 48. pp. 10 ProQuest Central; ProQuest Technology Collection. ISSN 08877661.

2 ARENDS R., AUSTEIN R., LARSON M., MASSEY D., a ROSE S., "DNS Security Introduction and Requirement," RFC 4033, Mar. 2005

3 ARENDS R., AUSTEIN R., LARSON M., MASSEY D., a ROSE S., "Protocol Modifications for the DNS Security Extensions," RFC 4035, Mar. 2005.

4 ARENDS R., AUSTEIN R., LARSON M., MASSEY D., a ROSE S., "Resource Records for the DNS Security Extensions," RFC 4034, Mar. 2005.

5 KENT S. a ATKINSON R., security Architecture for the internet Protokol, IETF Network Working Group RFC 2401, available at http://www.ietf. org/rfc/rfcl825.txt, November 1998.

6 KENT S. a ATKINSON R., IP Authentication Header, IETF Network Working Group RFC 2402, November 1998.

7 KENT S. a ATKINSON R., IP Encapsulating security Payload, IETF Network Working Group RFC 2406, November 1998.

8 GUTTMAN J. D., HERZOG A. L., a THAYER F. J., Authentication and Confidentiality via IPsec, Proceedings of the Sixth European Symposium on Research in Computer security - ESORICS 2000, Lecture Notes in Computer Science 1895, available at http://www.ccs.neu.edu/home/ gullman/esorics-ipsec.pdi, June 30, 2000.

IPsec má dva provozní režimy: Transportní režim a režim tunel. Při provozu v transportním režimu musí zdrojové a cílové stanice přímo provádět všechny kryptografické operace. Šifrovaná data jsou odeslána pomocí jednoho tunelu, který je vytvořen pomocí tunelovacího protokolu, který pracuje na druhé vrstvě.[2] Data (šifrovaný text) jsou vytvořeny zdrojovou stanicí a příjmuta cílovou stanicí. Tento mód zajišťuje „end-to-end" bezpečnost. Při režimu tunel provádějí kryptografické operace také koncové stanice, ale k nim navíc provádějí také tyto operace speciální brány. Zde je vytvořeno mnoho tunelů v sérii (nebo vnořené tunely) mezi bránami, které zajišťují bezpečnost brána-brána („gateway-togateway").[1] Při použití jakéhokoli módu je nutné, aby měli všechny brány možnost ověřit pravost paketu a autentifikovat paket na obou koncích. Každý nepravý paket je zahazován.[3][4]

Populární druh šifrování je šifrování s veřejným klíčem. Šifrovací klíč je veřejný a může ho využít kdokoli, nicméně dešifrovat zprávu může pouze ten, kdo má soukromý (neveřejný) klíč. Pokud uživatel A zašifruje zprávu pomocí veřejného klíče uživatele B, tak pouze uživatel B dokáže dešifrovat zprávu. Nikdo jiný, ani uživatel A, ji nedokáže

---

[1] PERLMAN R. a KAUFMAN C., Analysis of the IPSec Key Exchange Standard, Proceedings of the Tenth IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises- WET ICE 2001, available at http://sec.fenito.org/wetice-2001/papers/ radia-paper.pdf, 2001.

[2] SHINDER D., securing Data in Transit with IPsec, available at http://www.windowsecurity.com/ articles/Securing_Data_in_Transit_with_IPSec. html, Feb. 17, 2003.

[3] WU C.-L.,WU S. F., a NARAYAN R., IPSec/PHIL (Packet Header Information List): Design, Implementation, and Evaluation, Proceedings of the Tenth International Conference on Computer Communications and Networks, available at http://www.cs.ucdavis.edu/~wu/publications/ 314-PHIL.pdf, October 15-17, 2001.

[4] THOMAS, J. and ELBIRT, A.J. Understanding Internet Protocol Security. *Information Systems Security*, Sep, 2004, vol. 13, no. 4. pp. 39-43 ProQuest Central; ProQuest Hospital Collection; ProQuest Technology Collection. ISSN 1065898X.

dešifrovat. Jsou i jiné šifrovací systémy, které fungují na podobném systému. Všechny mají jedno společné, musí existovat dešifrovací klíč – typicky veliké číslo.[1]

SSL/TLS digitální certifikáty jsou používány k autentifikaci vlastnictví webové stránky a ostatních online zdrojů, tak i k šifrování informací kvůli soukromí, když informace prochází internetem a dalšími sítěmi.[2]

SSL/TLS certifikáty jsou kritickou částí internetové bezpečnostní infrastruktury, kombinují osvědčené technické standardy s možností škálování pro zacházení s milióny webových stránek a širokým polem uživatelských programů. Nové základní požadavky vylepší spolehlivost a zodpovědnost veřejně důvěryhodných autorit pro vydávání SSL/TLS certifikátů.[1]

Se základními požadavky budeme mít poprvé jednotný mezinárodní standard pro vydávání všech SSL/TLS, včetně mnoha variant ověření domény a organizace. To bylo mnohaleté úsilí více než 50-ti organizací včetně hlavních dodavatelů webových prohlížečů a CA autorit z celého světa, stejně jako zástupců z internetových standardů a auditorů/právníků spolu s hlavními souvisejícími stranami, které využívají SSL/TLS.[3]

Nový zásadní bezpečnostní test kontroluje, jestli mohou být DNS servery napadeny, jinými slovy jestli je možné do jejich vyrovnávací paměti (cache) uložit podvržené údaje. DNS spoofing může způsobit závažné bezpečnostní problémy pro firmy náchylné na tento typ útoku. DNS spoofing je reálná hrozba integrity aktivity na internetu, ať už komerční nebo nekomerční. Citlivost na DNS spoofing je pronikající – většina DNS serverů na internetu

---

1 HAMIS TECHNOLOGY LLC; Patent Application Titled "using Biometrics as an Encryption Key" Published Online. *Computers, Networks & Communications*, Nov 28, 2013. pp. 731 ProQuest Central; ProQuest Science Journals; ProQuest Technology Collection.

2 *CA/Browser Forum Approves Baseline Requirements for SSL/TLS Certificates.* Ottawa: , Dec 14, 2011 ProQuest Central.

3 WU C.-L.,WU S. F., a NARAYAN R., IPSec/PHIL (Packet Header Information List): Design, Implementation, and Evaluation, Proceedings of the Tenth International Conference on Computer Communications and Networks, available at http://www.cs.ucdavis.edu/~wu/publications/ 314-PHIL.pdf, October 15-17, 2001.

je náchylná na tento typ útoku. Úspěšný útok může způsobit vážné poškození v reputaci společnosti a jejím zákazníkům.[1]

SSL protokol je široce využíván v síťové bezpečnosti jako uživatelský účet, elektronická výměna dat, atd. Při útoku SSLStrip MITM vzniká problém s detekcí narušení a výkonem zpracování. Phishing, SSLStrip MITM a DNS spoofing jsou založené na myšlence sítě a vznikly z výše zmíněných důvodu. Bezpečnost SSL přihlášení v internetových službách byla také analyzována a byly dodány návrhy na zlepšení.[2]

Trojský kůň může pozměnit DNS server v nastavení sítě (TCP/IP) uživatelského počítače, aby ukazovalo na podvodné DNS servery (které typicky spravuje tvůrce trojského koně). V tomto případě každý uživatelův požadavek na DNS překlad, bude dotazován na podvodný DNS server. Tento server pak může být nakonfigurován, že bude posílat legitimní odpovědi až na jednu popř. více adres, například adresa www.nosuchbank.com bude přeložena na podvodnou adresu 10.20.30.40.[3]

Známá bezpečnostní řešení (jako antivirový program a antimalwarový program) jsou schopná zjistit, jestli hosts soubor nebo DNS konfigurace byla modifikována (nebo jsou nepřátelské), když jsou lokálně spuštěná. Tato řešení nejsou typicky schopná dodat adekvátní řešení pro poskytovatele internetu, a ostatní subjekty, kteří nemají takovýto přístup k počítačům svých klientů, a zároveň chránit tyto klienty společně se svými prostředky (propustnost sítě, redukce hovorů na zákaznickou podporu, zabezpečení) před trojskými koňmi.[1]

---

1 *DNS Expert 1.3 from Men & Mice Released; Crucial DNS Security Analysis for ISPs and DNS Administrators; Tests for DNS Spoofing and Mail Relay.* New York: , Dec 11, 1998 ProQuest Central.

2 ZHANG, Y.L. and XIA, G.S. The SSL MIMT Attack with DNS Spoofing. *Applied Mechanics and Materials*, 08, 2013, vol. 385-386. pp. 1647 ProQuest Technology Collection. ISSN 16609336. DOI http://dx.doi.org/10.4028/www.scientific.net/AMM.385-386.1647.

3 EMC Corporation; Patent Issued for System and Method for Detecting and Mitigating DNS Spoofing Trojans. *Computers, Networks & Communications*, Sep 27, 2012. pp. 2493 ProQuest Central; ProQuest Science Journals; ProQuest Technology Collection.

Za posledních deset let se velmi rozrostly phisingové útoky v internetu. Phishing spočívá v nalákání lidí na podvodnou stránku s cílem přesvědčit je, aby vyplnili důvěrné informace. Útočníci většinou udělají webovou stránku vizuálně podobnou reálné stránce, aby napálili uživatele. Slovo phishing je odvozené od slova „fishing“. Termín byl vytvořen hackery, kterým se podařilo ukrást účty America online (AOL) v roce 1995.[1] Toho času byly účty považované za „ryby“ a během roku byl „phish“ vyměňován mezi hackery jako forma elektronické měny, která pro ně měla hodnotu. Útočníci využívají napadené e-mailové účty k rozesílání nevyžádané pošty.[2]

Metodologie phishingu je velice podobná rybaření, kde je návnada vhozena s nadějí, že nic netušící uživatel ji chytí a zakousne se do ní stejně jako ryba. Proto je phishing také znám jako metoda návnady a háku.[3] Ve většině případů je návnada e-mail nebo chatovací stránka[4], která odkáže uživatele na nepřátelskou phishingovou stránku. Ve většině případů se jedná o kopii stránky nějaké banky. Podvodná stránka bude mít podobný vzhled jako původní stránka a bude žádat o vyplnění důvěrných informací jako uživatelské jméno, heslo, informace o kreditní kartě atd.[5] Jakmile oběť (uživatel) vyplní tyto údaje, jsou data odeslána útočníkovi, který je může využít k osobnímu zisku. Phishing se stal nejběžnějším

---

[1] JAMES L. (2006), "Phishing exposed. Tech target article sponsored by: Sunbelt software", available at: searchexchange.com.

[2] PURKAIT, S. Phishing Counter Measures and their Effectiveness - Literature Review. *Information Management & Computer Security*, 2012, vol. 20, no. 5. pp. 382-420 ProQuest Central; ProQuest Hospital Collection; ProQuest Technology Collection. ISSN 09685227. DOI http://dx.doi.org/10.1108/09685221211286548.

[3] EMM D. (2006), "Phishing update, and how to avoid getting hooked", Network Security, Vol. 2006 No. 8, pp. 13-15.

[4] SHENG, S., MAGNIEN B., KUMARAGURU P., ACQUISTI A., CRANOR L., HONG J. a NUNGE E. (2007), "Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish", SOUPS'07: Proceedings of the 3rd Symposium on Usable Privacy and Security, ACM, New York, NY, pp. 8899.

[5] HINDE S. (2004), "All you need to be a phisherman is patience and a worm", Computer Fraud & Security, Vol. 2004 No. 3, pp. 4-6.

kanálem pro zloděje, kteří získávají osobní informace, které jim pomáhají v krádeži identity.[1,2,3,4]

Organizace nejsou proti phishingovému útoku přes e-mail úplně bezbrané. Aby lépe ochránily zákazníky, nebo zaměstnance, mohou nastavit filtry pro klasifikaci e-mailů do dvou kategorií – legitimní a podvodné[5]. Coyotovo anti-podvodné centrum sídlící v Israeli zaměstnává třicet bezpečnostních analytiků. Každý den skenují jeden bilión e-mailů a hledají známky phishingu[6]. Využití těchto proaktivních organizací na scanování e-mailů může vyfiltrovat podezřelé phishingové e-maily a zabránit jejich doručení do cílové e-mailové schránky. Mnoho firem instaluje spam filtry, aby ochránily své zaměstnance. Jak je uvedeno ve studii Kenyon College, zavedení spam filtrů zastavilo velký počet pokusů o krádeže identity prostřednictvím e-mailů[7].

Case a King, při jejich výzkumu s vysokoškolskými studenty ze soukromé americké univerzity North Eastern zjistili, že 46% elektronické pošty obdržené studenty jsou podvodné e-maily[8].

---

1 MERCURI R.T. (2006), "Scoping identity theft", Communications of the ACM, Vol. 49 No. 5, pp. 17-21.

2 EISENTIEN E.M. (2008), "Identity theft: an exploratory study with implications for marketers", Journal of Business Research, Vol. 61 No. 11, pp. 1160-72.

3 BRODY R.G., MULIG E. a KIMBALL V. (2007), "Phishing, pharming and identity theft", Academy of Accounting and Financial Studies Journal, Vol. 11, pp. 43-56.

4 ANDERSON K.B., DURBIN E. a SALINGER M.A. (2008), "Identity theft", Journal of Economic Perspectives, Vol. 22 No. 2, pp. 171-92.

5 CASTILLO M.D., IGLESIAS A. a SERRANO J.I. (2007), "Detecting phishing e-mails by heterogeneous classification", in Yin, H. *et al.* (Eds), IDEAL 2007, LNCS, Vol. 4881, pp. 296-305.

6 KNIGHT W. (2005), "Caught in the net", IEEE Review, Vol. 51 No. 7, pp. 26-30.

7 MURPHY J.M. (2005), "The water is wide: network security at Kenyon College, 1995-2005", Proceedings of the 33rd Annual ACM Conference on User Services, SIGUCCS 2005, Monterey, CA, USA, pp. 237-40

8 CASE C.J. a KING D.L. (2008), "Phsihng for undergraduate students", Research in Higher Education Journal, Vol. 1, pp. 100-6.

1. Historie Internetu

S prvním návrhem globální sítě přišla společnost RAND (americké mozkové centrum za dob studené války), která se snažila vymyslet způsob jak zajistit komunikaci mezi jednotlivými státy, městy apod. v případě nukleárního útoku. V šedesátých letech společnost RAND ve spolupráci s americkými univerzitami (MIT, Los Angeles UCLA) vytvořila testovací síť v národní fyzikální laboratoři ve Velké Británii. Na to přišla americká agentura pro pokročilý výzkum (ARPA) s ještě větším projektem vybudovat celosvětovou síť (ARPANET). Uzly této sítě tvořily velmi výkonné superpočítače, v roce 1969 byly zprovozněny první 4 uzly na síti. V roce 1971 měla síť ARPA 15 uzlů na celém světě, další rok to pak bylo 37 uzlů.

Původním záměrem ARPANETu bylo sdílení výpočetního výkonu, kterého v té době nebylo nazbyt. Po pár letech ARPANETu se síť začala využívat i k dalším věcem jako je sdílení informací a posílání osobních zpráv. Každý uživatel ARPANETu měl svou vlastní schránku pro elektronickou poštu, díky které si mohli posílat pracovní zprávy (například při konzultaci na nějakém projektu). Po čase se síť začala používat ať pro komunikaci (osobní i pracovní) namísto vzdáleného počítání. Díky využívání sítě ke komunikaci byl vymyšlen *mailing-list*, ten sloužil k hromadnému odesílání jedné zprávy více lidem najednou. Díky necentralizované topologii sítě se v 70. letech síť velice rychle rozrůstala. Jedinou podmínkou připojení do sítě bylo, aby počítače rozuměly paketově orientovanému protokolu sítě (v té době *Network Control Protokol* (NCP)), na ničem jiném nezáleželo.

V průběhu 70. a 80. let se staly superpočítače více dostupné, než byly dříve a díky tomu se začaly připojovat další subjekty k síti. Díky přechodu na protokol TCP/IP se začaly připojovat i celé sítě a ARPANET zaujímal stále menší část, proto se celá síť označovala jako „sítě-sítí“. Později se již začalo užívat označení internet.

Připojování k internetu nestálo vůbec nic, protože si každý uzel musel zajistit finanční zabezpečení a technické vybavení. V roce 1984 se k síti přidala i národní vědecká nadace (NSF), která stála za vývojem sítě NSFNET, díky které se zrychlilo tempo zdokonalování linek a přepojování na novější výkonnější superpočítače, síť NSFNET dodnes funguje jako hlavní páteř pro komunikační služby a Internet ve Spojených státech. K Internetu se

připojovaly i vládní agentury, které se snažili přispět ke zlepšování infrastruktury a páteřní sítě Internetu.

Síť ARPANET oficiálně zanikla v roce 1983. Uživatelé sítě ARPANET to ani nezaznamenali, protože veškeré služby dále fungovaly a nadále se zlepšovaly. Protokol TCP/IP se začal využívat po celém světě při vytváření počítačových sítí. V dnešní době má Internet kolem 4 milionů uzlů rozprostřených mezi 40 000 sítěmi.

1.1 Historie Internetu v ČR

V roce 1988 byl první pokus připojit vysoké školy v ČR do evropské akademické výzkumné sítě (EARN), tento pokus se nezdařil. Připojení vysokých škol do sítě EARN se uskutečnilo v roce 1990, kdy byl vybudován pevný spoj mezi Prahou a Lincem o kapacitě 9,6 kb/s (uzel byl na ČVUT). O rok později byla kapacita linky zdvojnásobena, linka se rozdělila na 2 nezávislé kanály. Jeden sloužil pro komunikaci v síti EARN a druhý sloužil pro připojení k internetu.

V roce 1991 na základě zájmu akademické komunity byl iniciován projekt FESNET (*Federal Education and Scientific NETwork*). Po rozdělení republiky byl tento projekt modifikován na CESNET (*Czech Scientific and Education NETwork*) v ČR a SANET (*Slovenská Akademická a datová síť*) v SR. Ministerstvo upravený projekt schválilo a počátkem roku byla síť CESNET uvedena do provozu. Infrastruktura sítě je zobrazena na obrázku 1.

Obrázek 1: Síť CESNET v roce 1993
Zdroj: http://www.cesnet.cz/sdruzeni/dokumenty/historie-narodni-site-pro-vedu-vyzkum-a-vzdelavani/

Všechny spoje kromě páteřního spoje Praha – Brno měly kapacitu 19,2 Kb/s, páteřní spoj Praha – Brno měl kapacitu 64 Kb/s. Díky velkému zájmu o připojení k internetu začali kapacity jednotlivých spojů rychle stoupat. Síť CESNET nebyla pouze síť pro univerzity a vysoké školy, ale začala připojovat i komerční subjekty. Přehled navyšování kapacit spojů je vyobrazen v tabulce 1.

Rok	Kapacita páteře Praha-Brno	Kapacita ostatních spojů
1993	64 Kb/s	19,2 Kb/s
1997	34 Mb/s	34 Mb/s
1999	155Mb/s	34 Mb/s

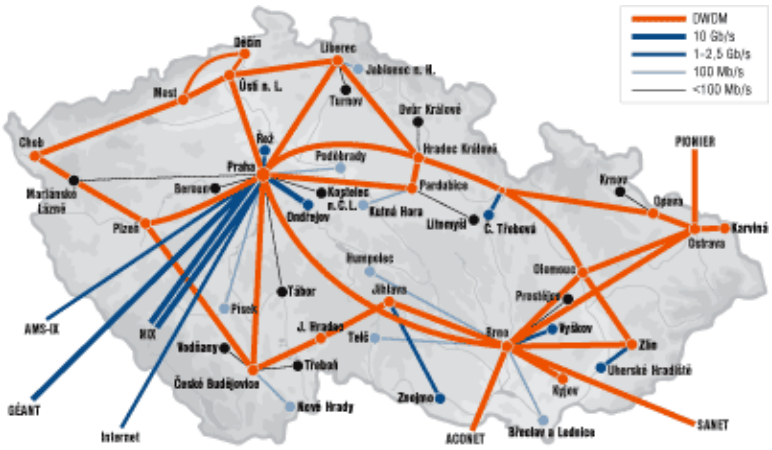
Tabulka 1: Vývoj kapacit spojů sítě CESNET
Zdroj: vlastní zpracování podle http://www.cesnet.cz/sdruzeni/dokumenty/historie-narodni-site-pro-vedu-vyzkum-a-vzdelavani/

V roce 2000 se CESNET rozhodl ukončit poskytování komerčních služeb, protože se chtěl věnovat výlučně rozvoji sítě pro vědu, vzdělání a výzkum, síť prodal firmě Contactel, která ji začlenila do své infrastruktury. V roce 2000 byl v evropské unii (EU) projekt GÉANT, díky kterému se začínaly budovat spoje o přenosové kapacitě 1 Gb/s. Takovýchto přenosových kapacit se dosáhne na velké vzdálenosti pouze za použití optického vlákna. Kvůli vysokým finančním nákladům se využil přístup CEF (*Customer Empowered Fibre Network*). Jedná se o natažení optických vláken, a následné oživení si provede sám zákazník až v případě, že na to má potřebnou technologii, znalosti a finance. Tento postup se využil při budování další akademické sítě, která byla v říjnu 2001 pojmenována jako CESNET2 .

Tato síť měla od roku 2002 několik spojů s přenosovou kapacitou 1 Gb/s. V roce 2004 se začalo s nasazováním nových technologií (např. DWDM), které umožňovaly další navýšení přenosové kapacity. Během dvou let síť CESNET2 vybudovala uzavřený okruh (Praha – Brno – Olomouc – Hradec Králové) na technologii DWDM, který je zobrazen na obrázku 2.

Obrázek 2: Infrastruktura sítě CESNET2 v roce 2005
Zdroj: http://www.cesnet.cz/sdruzeni/dokumenty/historie-narodni-site-pro-vedu-vyzkum-a-vzdelavani/

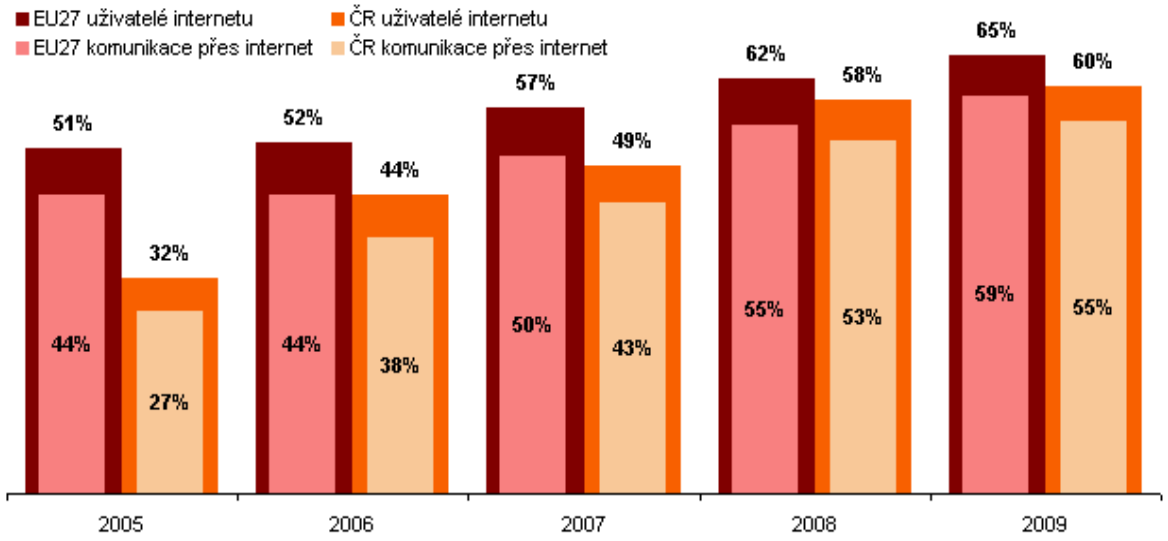
Ke konci roku 2010 měla síť CESNET2 roztaháno více než 4000 km optických vláken na technologii DWDM. Infrastruktura sítě z roku 2010 je zobrazena na obrázku 3.



Obrázek 3: Infrastruktura sítě CESNET2 v roce 2010
Zdroj: http://www.cesnet.cz/sdruzeni/dokumenty/historie-narodni-site-pro-vedu-vyzkum-a-vzdelavani/

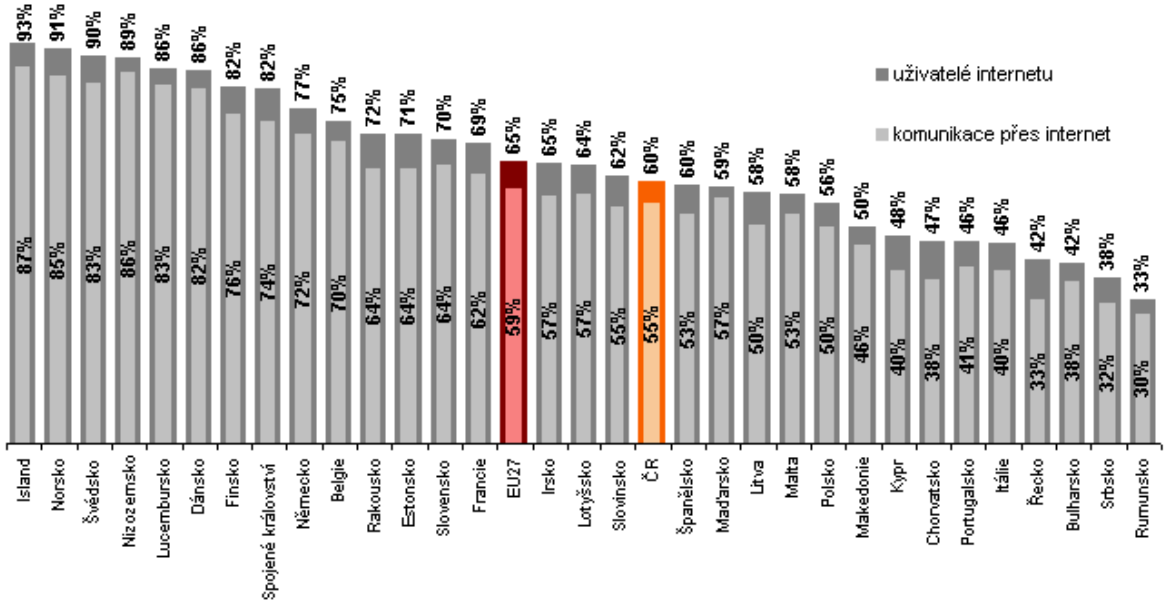
2. Trendy Internetu

Trendy internetu v České republice a ve světě dají odvodit podle jeho dosavadního vývoje. Vezmeme-li v úvahu například síť CESNET(2), která byla schopná se během 20-ti let dostat od původních spojů s přenosovou kapacitou 9 kb/s až po komplexní páteřní spoje na technologii DWDM. Díky takovýmto vylepšením jednotlivých spojů jsou poskytovatelé internetu sto dostat ke koncovým uživatelům daleko větší kapacity než dříve, čímž umožňují uživatelům lépe využívat jednotlivé služby, ať už pro zábavu (například sledování internetové televize (IPTV)), nebo pro komunikaci (například telefonie přes internet (VoIP), posílání e-mailů, využívání diskusních fór, atd.). V České republice se během let 2005 – 2009 zdvojnásobil počet uživatelů, kteří využívají komunikaci přes internet (více Obrázek 4).



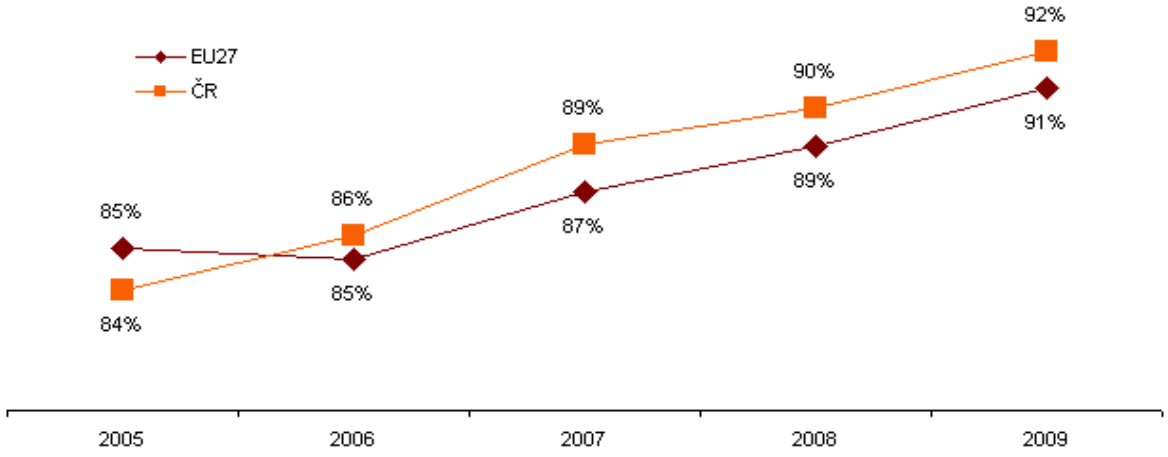
Obrázek 4: Používání internetu a komunikace přes internet v letech 2005 – 2009
Zdroj: Eurostat, Community survey on ICT usage in households and by individuals, 2010

V Evropě se nejvíce využívá internet v severních státech, jako jsou Island, Norsko, Švédsko, naopak nejméně se internet využívá v jihovýchodní a jižní Evropě (Řecko, Bulharsko, Rumunsko). Celkové využití je vidět na obrázku 5.



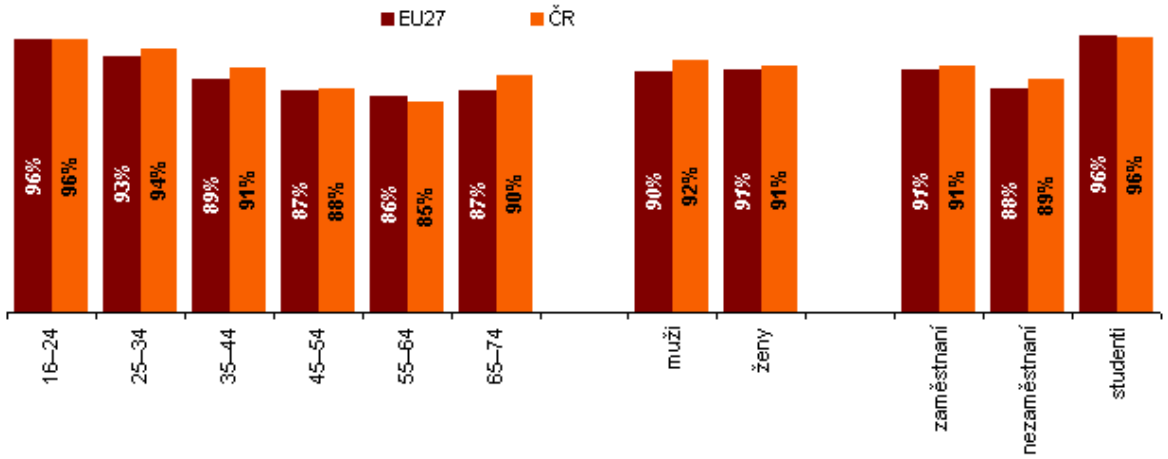
Obrázek 5: Využití Internetu a internetové komunikace v Evropě v roce 2009
Zdroj: Eurostat, Community survey on ICT usage in households and by individuals, 2010

Na obrázku 6. je zobrazeno procentuální využití internetové komunikace (elektronická pošta, chat, diskusní fóra, …) v České republice mezi lety 2005 – 2009.



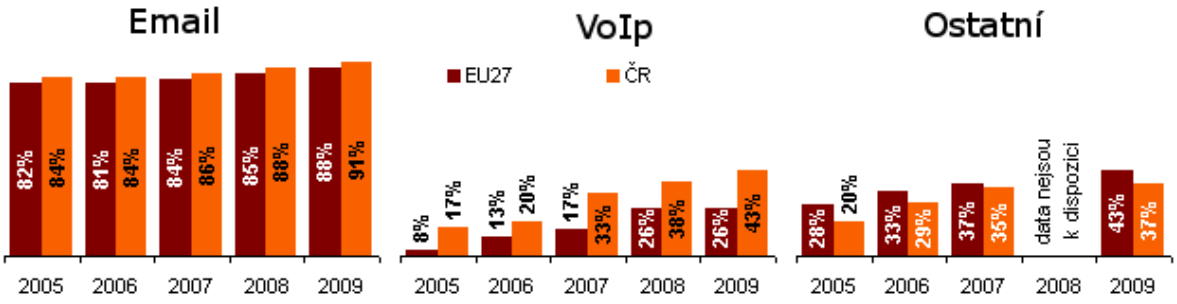
Obrázek 6: Využití komunikace přes Internet
Zdroj: Eurostat, Community survey on ICT usage in households and by individuals, 2010

Využívání internetové komunikace velice záleží na mnoha faktorech (věk, zaměstnání, pohlaví). Podrobnější využití internetové komunikace je vyobrazeno na obrázku 7., kde je dané využívání internetové komunikace rozděleno do více skupin.



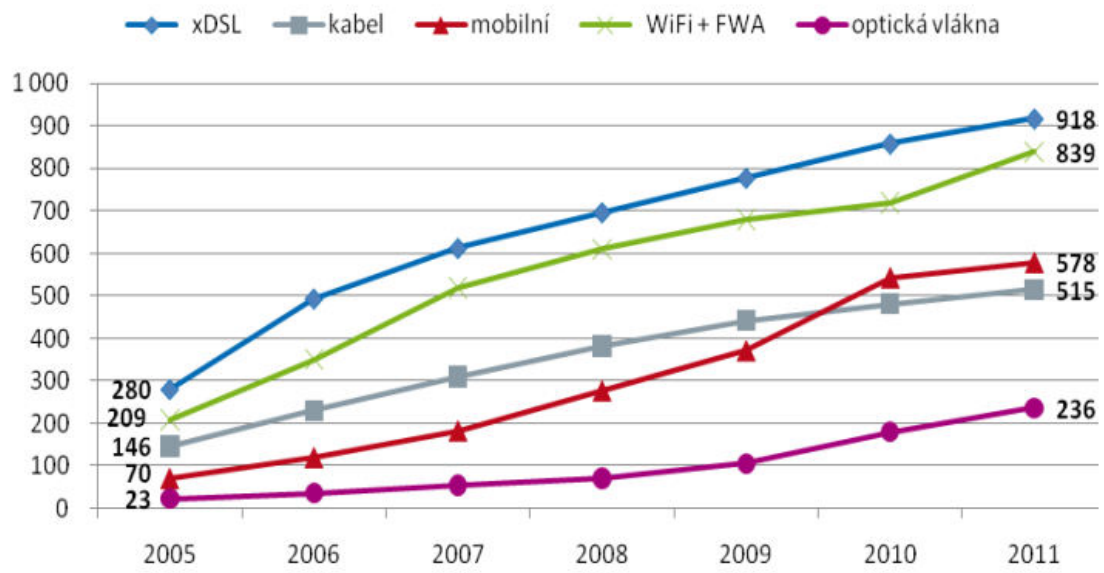
Obrázek 7: Rozdělení využití Internetové komunikace do více skupin
Zdroj: Eurostat, Community survey on ICT usage in households and by individuals, 2010

Nejvíce využívanou formou komunikace je elektronická pošta, v České republice ji využívalo v roce 2009 celkem 91% uživatelů, dále se hojně využívala telefonie přes internet (VoIP). Ostatní formy komunikace (chat, diskusní fóra, blogy, sociální sítě, …) v této době ještě nebyly moc oblíbené, i přesto si nacházejí čím dál tím víc uživatelů. Porovnání jednotlivých druhů komunikace v letech 2005 – 2009 je vyobrazeno na obrázku 8.



Obrázek 8: Způsoby komunikace přes Internet
Zdroj: Eurostat, Community survey on ICT usage in households and by individuals, 2010

Důvodem k nárustu využívání internetové komunikace je také kvalitnější způsob připojení k internetu pro koncové uživatele. Na obrázku 9. je zřetelné, že od roku 2008 respektive 2009 dochází k velkému nárustu uživatelů připojenýnch optickým vláknem, což je v dnešní době nejkvalitnější připojení k internetu. Dále je vidět obrovský skok v mobilním připojení v roce 2010.



Obrázek 9: Technologie připojení k internetu (v tisících)
Zdroj: Český statistický úřad

Z obrázku 9 se dá odhadnout i budoucí trend připojení k internetu – budou se čím dál více používat kvalitnější typy připojení (optické vlákno, kabel, …) a budou pomalu mizet méně kvalitní způsoby připojení (Wi-Fi, respektive Wi-Fi s frekvencí 2.4 GHz, která se v dnešní době už moc nevyužívá, protože toto pásmo bylo velice zarušené – méně kvalitní přenos dat). Díky vysokému rozšíření chytrých telefonů, se dá také předpokládat, že bude nadále růst zájem o mobilní připojení, jelikož chytré telefony bez připojení k internetu více méně ztrácejí svůj význam. Mobilní připojení se neustále vyvíjí a přenosové rychlosti se neustále navyšují.

3. Webové stránky

Vzhledem k tomu, že se jedná o aplikace související s webem, je pokládáno za vhodné zde uvést do problematiky tvorby webových stránek. Webové stránky jsou děleny na dynamické a statické, jak již bylo uvedeno výše. V následující kapitole budou ukázány základy jazyků HTML, CSS, PHP a popsány rozdíly mezi statickými a dynamickými stránkami.

3.1 Statické webové stránky

Statické webové stránky, jsou stránky, jejichž obsah je neměnný. Pro vytváření tohoto typu webových stránek postačí programátorovi základní znalosti jazyka (X)HTML ideálně ve spojení s jazykem CSS pro upravení vzhledu dané stránky. Problém ovšem nastane, jakmile by chtěl programátor provést nějakou změnu. Dané změny by musel provádět přímo ve zdrojovém kódu dané stránky. Jako příklad lze využít datum, jež se zobrazuje na stránkách. Pokud by byl datum zadán na statickou webovou stránku, bylo by nutné, aby jej programátor každý den ručně měnil. Nezná-li programátor jazyk (X)HTML, tak dané změny nejspíše neudělá, a pravděpodobně napáchá více škod než užitku.

Kód statické stránky může vypadat nějak takto:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="cs" lang="cs">
     <head>
          <meta http-equiv="content-type" content="text/html; charset=utf-8">
          <title>Statická stránka</title>
     </head>
     <body>
          <h1>Toto je statická stránka</h1>
     </body>
</html>
```

3.2 Dynamické webové stránky

Dynamické webové stránky zjednodušeně řečeno oživí statické stránky. Stránky budou reagovat na uživatelovy požadavky.

Dynamické webové stránky umožňují programátorovi přebírat z formulářových polí data, s nimiž dále pracuje (ukládá je do databáze, odesílá je e-mailem, vyhledává podle nich v databázích, apod.). Tyto stránky umožňují dynamicky měnit barvu pozadí podle výběru uživatele, chatovat a další věci. Ke statickým (X)HTML stránkám se přidá např. PHP, JS kód a hned získává programátor daleko větší možnosti. Při použití základní funkce v PHP může programátor jednoduše měnit obsah elementů ve stránce (např. elementu `<div>`), tím zamezí načítání celé stránky, což zrychluje načítání stránky. To samé se dá samozřejmě udělat při použití jakéhokoli jiného skriptovacího jazyka.

Kód dynamické stránky:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="cs" lang="cs">
     <head>
          <meta http-equiv="content-type" content="text/html; charset=utf-8">
          <title>Dynamická stránka</title>
     </head>
     <body>
          <h1>Toto je dynamická stránka stránka</h1>
          <p>Dnes je <?= date("d.m.Y") ?></p>
     </body>
</html>
```

Stránky se stávají dynamickými právě díky zápisu: <?= date(“d.m.Y“) ?>, který do stránky vypíše aktuální datum, a majitel stránky ho tak nemusí každý den ručně vpisovat přímo do zdrojového kódu stránky.

4. Právo a internet

Vzhledem k tomu, že se síťová informační infrastruktura začala původně vyvíjet ve Spojených státech amerických, přebírá celosvětová informační síť do značné míry tamější organizační modely. USA jsou přitom zemí, kde mají hluboké kořeny myšlenkové směry jako liberalismus či dokonce libertariánství. Jednou ze základních myšlenek liberalismu je odstranění nejrůznějších forem regulace omezující jednotlivce v realizaci jejich záměrů a dosažení odpovídajícího prospěchu, ať už materiálního či jiného.[1]

Každý stát má jiné zákony, co se týká internetu respektive kyberprostoru. Organizace Electronic Frontier Foundation (EFF) podporuje hnutí za svobodný internet. Již od svého založení v roce 1990 se tato organizace snaží vypomáhat v soudních sporech, v případech právního omezování svobody jedince na internetu. EFF se řídí tzv. „Deklarací nezávislosti kyberprostoru“[2].

Deklarace obsahuje několik argumentů, proč by se neměla svoboda na internetu jakkoli regulovat. Jsou to například:

- Neexistence smlouvy mezi adresáty právních norem a jejich tvůrcem (státem)
    - Založeno na předpokladu, že na internetu vzniká nové společenství
- Řada problémů zmiňovaných jako důvodů k regulaci neexistují.
    - Pokud jsou nějaké problémy, internetové společenství má veškeré prostředky i snahu nezbytné k jejich řešení.
- Neschopnost států uzavřených v tradičně prostorových hranicích jurisdikce efektivně vynucovat právo.
    - Stát nemá prostředky na to jak adresáty norem donutit, aby se podle nich chovali

[1] POLČÁK R., *Internet a proměny práva*. [2012], strana 95

[2] Deklarace je dostupná online na adrese: www.homes.eff.org/~barlow/Declaration-Final.html

4.1 Příklady vymáhání práva na internetu

Policie ČR v roce 2001 odložila případ trestného činu pomluvy s odůvodněním, že se uskutečnil na internetovém diskusním fóru. Vyšetřovatel nezjišťoval všechny potřebné věci. Toto rozhodnutí pak napadal tehdejší ministr spravedlnosti. Nejvyšší soud ČR žádosti vyhověl a vyšetřovateli poskytl návod, jak postupovat. Z nálezu vybíráme: „Podstata porušení zákona v daném případě spočívá v tom, že vyšetřovatel učinil rozhodnutí o zastavení trestního stíhání obviněného z výše uvedeného důvodu, aniž náležitě zjistil skutkový stav a provedl veškeré dostupné důkazy, které se v této věci nabízely. […] Dále bylo třeba vyžádat znalecký posudek z oboru výpočetní techniky se zaměřením na software a provést příslušné zkoumání zajištěných internetových stránek nalézajících se pod internetovou adresou, jakož i zřízené internetové stránky na jméno Z. S., s cílem získat údaje směřující k identifikaci osoby, která uvedené stránky a schránku zřídila, včetně údajů, které by umožnily určit osobu, jež předmětný pomlouvačný text na tyto stránky umístila.“ [1,2]

V Číně se stal typově podobný případ, kde se jednomu jedenačtyřicetiletému Qui Chenwengovi, hráči oblíbené on-line hry, podařilo získat pro svou postavu dračí meč. Ten meč pak půjčil svému kamarádovi, který ho prodal za 7200 juanů (necelých 20 000 Kč). Při oznámení tohoto činu bylo Quiovi oznámeno, že se na virtuální vlastnictví zákony nevztahují a policie to nebude řešit, Qui byl tak rozezlen, že svého kamaráda několika bodnými ranami usmrtil. Za tento čin pak dostal trest smrti, který byl později zmírněn na doživotní vězení.[1]

[1] POLČÁK R., *Internet a proměny práva.* [2012], strana 105

[2] Rozsudek nejvyššího soudu ze dne 16. 1. 2001, č. j. 4 TZ 265/2000. Dostupné online z www.nsoud.cz

4.2 Právo na internetu a mezinárodní spolupráce

Vedle dobrovolné či vynucené kooperace definičních autorit se k zajištění faktické realizace právních pravidel nabízí využití možností mezinárodní spolupráce. Na výše uvedených praktických příkladech demonstrované pozitivní či negativní konflikty pravomocí jsou společně s fenoménem definičních autorit důvodem, proč se současné právo stále nemůže zbavit výše uvedeného třetího argumentu.[1]

Další problém, krom toho, že by státy nebyly ochotny popřípadě efektivně vymáhat právo, je občasné překrývání jejich faktických (technické) i formálních (právní) kompetencí, popřípadě se kompetence vůbec nedotýkají.

Obecné srovnání faktických forem, v nichž je právo na internetu pod národními jurisdikcemi uplatňováno, pak je vzhledem ke komplexnosti materie prakticky nemožné a vznikají tak jen dílčí studie zaměřené na konkrétní aspekty práva ICT, nebo dokonce i jen na konkrétní řešené případy.[1]

Z předchozích argumentů by se mohlo zdát, že mezinárodní spolupráce co se týká vymáhání práva na internetu je téměř nemožná. Naopak je to jedna z podmínek vymáhání práva na internetu. Klíčem k úspěchu mezinárodní spolupráce v nastolení efektivní působnosti práva na internetu tedy není ve svém důsledku nic menšího než potlačení státní suverenity a přijetí a spolehlivá ochrana cizí jurisdikce.[2]

Při mezinárodní spolupráci při vymáhání práva platí jednoduché pravidlo – čím je právem chráněný zájem závažnější tím je mezinárodní spolupráce složitější. Z tohoto důvodu je nutné nenahlížet na právo jako na jeden celek, ale rozdělit jej na více oborů a to trestní, správní a soukromé právo.

---

[1] POLČÁK R., Internet a proměny práva. [2012], strana 112

[2] Srov. např. TRACHMAN, J. Cyberspace, Modernism, Jurisdiction and Soveregnity. Indiana Journal of Global Legal Studies. 1998, roč. 5, č. 2, strana 577

4.2.1 Trestní právo a mezinárodní spolupráce

Trestní právo chrání především vitální zájmy státu a společnosti. Z tohoto důvodu platí princip neoddělitelnosti otázky jurisdikce a rozhodného práva – jinými slovy, trestní soud, je-li příslušný k rozhodnutí ve věci, rozhoduje vždy podle práva svého státu. Uvedené platí i naopak – vztahuje-li se tedy trestní právo hmotné určitého státu na nějaký skutek, znamená to, že o skutku může rozhodnout i soud tohoto státu.[1]

Prakticky lze stíhat trestné činy na území státu nejen, kde se trestný čin odehrál, ale také na území státu (popřípadě států), na které měl daný trestný čin nějaký vliv. I v ČR je několik případů, při kterých je možné stíhat pachatele, který se nachází v době spáchání trestného činu mimo republiku. Díky tomu, že většina vyspělých států má obdobnou trestní legislativu jako ČR dochází u tzv. „mezinárodních internetových trestních činů" ke stíhání pachatele na území více států. V internetové trestné činnosti jsou nejčastější případy, kdy se trestný čin stane na území jednoho státu, přitom následky daného činu ovlivní stát jiný. V takovém případě je možné stíhat pachatele ve všech dotčených státech, bohužel je tato situace příznivá spíše pro pachatele než pro orgány činné v trestním řízení, a to zejména protože je prošetření a provedení veškerých potřebných úkonů otázkou komplikované mezinárodní spolupráce i navzdory tomu, že se jednotlivé soudní orgány snaží spolupracovat. Spolupráci často brání složité procesní postupy a rozdílné legislativy. V případech, kdy hlavní roli při zadržování důkazů hraje čas, je v podstatě nemožné pachatele usvědčit.

4.2.2 Správní právo a mezinárodní spolupráce

„Zatímco trestní i soukromé právo se mají možnost při vyrovnávání se s nově nastolenými problémy internetové jurisdikce opřít o více či méně tradiční mechanismy a principy, správní právo bylo s příchodem společenských vztahů nové kvality zastiženo náhle a překvapivě. Normy a instituce správního práva tak neměly až na výjimky možnost

[1] AKEHURST, M. Jurisdiction in Internation Law. In British Yearbook of International Law, London: Oxford University Press, 1972-1973, strana 179 a následující.

postupně si zvykat na existenci vztahů, jejichž aspekty nutí státní orgány uvažovat v mezinárodním měřítku, neboť jednoduchá konstrukce takových vztahů tj. adresát-orgán, tento postup nikdy přímo nevyžadovala.“[1]

Problém delokalizace je vidět hlavně v oboru finančního práva, kde je problém určení místa zdanitelného plnění a domicity internetových transakcí. Pachatelé trestné činnosti mohou přesouváním mezi jednotlivými jurisdikcemi popř. umístěním mimo jurisdikce unikat postihům. Stejně tak se mohou vyhýbat zdanění. Stejný problém je i v otázkách loterijního práva. V současné Evropě probíhají spory o správní jurisdikci sázkových kanceláří. Z toho se dá usuzovat, že budou vznikat další mezinárodní administrativně-právní konflikty. Sázková činnost je v každém státu brána trochu jinak, někde jde například o monopol, jinde o volnou koncesi. Díky internetu tyto věci ne zcela platí, v případě, že se sázková společnost usadí v zemi, kde je administrační regulace na nízké úrovni a bude nabízet své služby na internetu, tak může oslovit jak uživatele ve státě, kde podniká, ale i uživatele ve státě, kde je sázková činnost monopolem. Každý stát se proti tomu brání různě, v ČR se ministerstvo financí vydalo cestou národní soudní ochrany[2], Francie a Nizozemsko zvolily podobné řešení.

Problémy efektivity práva okolo internetového sázení se hromadí již několik let a přitom je státy stále nedokáží ani přes veškeré úsilí uspokojivě řešit. Z toho je patrné, že řešení regulace sázení na internetu a jakákoli jiná regulace na internetu není otázkou pro jednotlivé státy, ale pro širší mezinárodní spolupráce. Taková spolupráce by eliminovala místa, která jsou vůči těmto věcem benevolentní. V případě, že by byla jednotná pravidla pro internetové sázení a činnost internetových sázkových kanceláří, dá se očekávat, že státy jako Malta, Kypr by se díky nevoli ostatních států zřekly své benevolentnější úpravy, díky které bohatě těží.

[1] POLČÁK R., Internet a proměny práva. [2012], strana 120

[2] V ČR nejsou právnické osoby trestně odpovědné

4.2.3 Soukromoprávní otázky a mezinárodní právo

Oproti trestnímu právu, které se stará o vitální zájmy státu se soukromoprávní právo stará o ochranu soukromých zájmů subjektů jednajících ve vzájemně rovném postavení. Rozdíly mezi trestním a soukromým právem lze vnímat i v oblasti mezinárodní deliminace místní působivosti práva. V soukromém právu totiž dochází k oddělení procesního práva, hmotného práva a otázek příslušnosti. Oproti tomu v trestním právu se používá jeden hraniční určovatel k založení pravomoci a příslušnosti soudu, tak i k založení působnosti hmotného trestního práva.

Působnost soukromého a hmotného práva je poněkud benevolentnější, protože strany mají v některých případech možnost vymanit se z dosahu hmotného i procesního práva pomocí vzájemného ujednání.

„Struktura kolizního práva je u členských Evropské unie tvořena v oblasti procesní především nařízením Rady (ES) č. 44/2001 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech, a v oblasti hmotného práva pak Římskou úmluvou o právu rozhodném pro mimosmluvní závazkové vztahy (Řím II).“[1]

V otázkách mezinárodní spolupráce je na tom soukromé právo nepoměrně lépe než v otázkách trestního popřípadě správního práva. Na rozdíl od trestního a správního práva, kde státy odmítají omezit vlastní suverenitu ve prospěch působnosti vlastního práva, zde to takový problém není, přes to všechno ale není mezinárodní spolupráce v otázkách soukromého práva úplně bez problému. Soukromé právo je neefektivní v případech internetových soukromoprávních transakcích, protože doposud nebyly legislativně upraveny ani doktrinálně podchyceny specifické hraniční určovatele pro prostřední informační sítě.

[1] BOGDAM, M. Torts in Cyberspace: The impact of the New Regulation Rome „II“. MUJLT. 2009, roč. 2, č.1, strana 2

4.3 Definiční autorita

Definiční autorita je organizace, které tvoří internetové standardy a směrnice. „Definiční autority povahou připomínají ve mnoha směrech bohy z antické mytologie. V antické mytologii se bohové odlišují od lidí tím, že mají schopnosti ovládat přírodní síly, definiční autority mají podobné schopnosti, ale ty ovládají prostředí pomocí svých definičních norem. Například provozovatel on-line hry definuje pravidla hraní, částečně i obsah herního prostředí. Definiční autority sice, podobně jako Ovidiovi bohové, nemohou přímo definovat chování lidí. Mají však moc toto chování ovlivňovat na úrovni charakteristik prostředí. Ani bohové tak člověku nemohli například zabránit v rouhání – pokud tak činil, mohl jej však zbavit řeči. Podobně provozovatel diskusního serveru nemůže přímo zabránit účastníkům debaty v tom, aby se vzájemně neuráželi – může však automaticky mazat diskusní příspěvky nebo dokonce vybraným diskutujícím zcela zablokovat aktivní přístup.“[1]

Kompetence jednotlivých autorit jsou rozděleny do několika vrstev. Je tedy možné, že se hranice působnosti dvou či více definičních norem prolínají. Například výše zmíněný případ diskusního serveru, provozovatel může mít pronajaté místo v serverovně pro umístění serveru u nějakého poskytovatele internetových služeb, ten si může odkupovat konektivitu do internetu atd. Z toho vyplývá, že majitel diskusního serveru není jediný, kdo rozhoduje o existenci daného serveru, ale částečně i ISP u kterého má server umístěn, ISP od kterého odkupuje konektivitu do internetu, dodavatel energie, a další.

Poslední společný znak mezi definičními autoritami a Ovidiovými bohy je forma jejich existence. Na první pohled bohové vypadali jako lidé, čehož využívali při různých interakcích s lidmi, stejně tak je srovnatelná forma definičních autorit s formou subjektů, kterým tyto autority vytvářejí a spravují existenční prostor. Většina definičních autorit má proto formu fyzických případně právnických osob. Forma je důležitá zejména pro definiční autority na internetu, forma právnické či fyzické osoby může mít pro autority dalekosáhlé

[1] POLČÁK R., Internet a proměny práva. [2012], strana 138

následky. Zejména subjektivizace definičních autorit vůči právu (zjednodušeně z definičních autorit před právem stávají „smrtelníci“).

4.4 Pojem ISP

„Jak bylo uvedeno výše, mají definiční autority v mnoha směrech de facto specifické postavení. Veškeré dění v informačních sítích probíhá prostřednictvím infrastruktury či služeb, a disponují tedy faktickým a vysoce efektivním regulačním potenciálem. Na druhou stranu však mají charakter běžných subjektů práva a státy nad nimi tedy mohou vykonávat svou jurisdikci.“ [1]

Definiční autority mají zvláštní postavení prostřednictvím institucionalizace a právní úpravy postavení vybraných typů. Zavedením pojmu poskytovatel služeb informační společnosti (ISP – information service provider) je základním momentem specifické právní regulace definičních autorit. Jednoduše řečeno zahrnuje takové definiční autority pomocí kterých probíhá tvorba zpracování případně výměna informací.

ISP neobsahuje všechny definiční autority, ale jen ty které poskytují služby ostatním, většinou za nějakou úplatu. Pojem informační služba je v EU definován směrnicí č. 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů ve znění směrnice č. 98/48/ES. V této směrnici není definován samotný pojem ISP, ale jen pojem služby informační společnosti a to v podstatě jen okrajově, nicméně z ní vychází definice služby informační společnosti do dalších oblastí evropského i národního práva.

Vymezení pojmu služby informační společnosti dle novelizovaného článku 1(2):

„Službou informační společnosti se rozumí jakákoli služba informační společnosti, tj. každá služba poskytovaná zpravidla za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb.“[1]

[1] POLČÁK R., Internet a proměny práva. [2012], strana 140

- „poskytováno na dálku“ – poskytování bez současné přítomnosti obou stran
- „poskytováno elektronicky“ – služba odesílaná z místa A do místa B využitím elektronického zařízení a jako celek odesílána (drátově, rádiově, opticky nebo jiným elektromagnetickým přístrojem).

Do tohoto ustanovení čl. 1(2) směrnice č. 98/34/ES spadají i výjimky vymezené v příloze č. 5 a jsou následující:

1. Služby, které nejsou poskytovány „na dálku“
   Služby poskytované za osobní přítomnosti poskytovatele a příjemce, a to i tehdy, použije-li se přitom elektronické zařízení:
   a. Lékařská vyšetření nebo ošetření v lékařské ordinaci za použití elektronického zařízení a za osobní přítomnosti pacienta;
   b. Prohlídka elektronického katalogu v prodejně za přítomnosti zákazníka;
   c. Rezervace letenek pomocí počítačové sítě v cestovní kanceláři a za osobní přítomnosti zákazníka;
   d. Zpřístupnění elektronických her v herně za osobní přítomnosti uživatele.
2. Služby, které nejsou poskytovány elektronicky
   Služby materiální povahy, ačkoli jsou poskytovány elektronickými přístroji:
   a. Stroje pro automatický výdej peněz nebo lístků (bankovky, jízdenky);
   b. Vstup do silničních sítí, na parkoviště apod. podléhající poplatkům, a to i tehdy jsou-li v místě vjezdu instalována elektronická zařízení kontrolující vstup a/nebo zajišťující řádné zaplacení,
      i. služby poskytované off-line: prodej kompaktních disků nebo programového vybavení na disketách
      ii. služby, které nejsou poskytovány elektronickými systémy pro zpracování/ukládání dat:
         1. hlasové telefonní služby;
         2. telefaxové/telexové služby;
         3. služby poskytované hlasově po telefonu nebo faxem
         4. lékařské porady po telefonu/telefaxu

5. právnické porady po telefonu/telefaxu
6. přímí prodej po telefonu/telefaxu[1]

Právní definice ISP byla v EU zavedena až směrnicí č. 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu. Definice je, dá se říci jen odkaz na výše uvedenou směrnici.

4.5 Vývoj práva v ČR

Česká právní věda není založena na sovětské doktríně, tudíž nedošlo k pokusu výstavby strojů na právo, které by automatizovaně řešily otázky zákonnosti, za předpokladu správného nakódování. Díky tomu u nás měla právní informatika hned od počátku spíše podpůrný a instrumentální charakter a to kvůli pragmatickému zhodnocení tehdejších možností využití kybernetických metod v právu.

Velkou roli v oblasti informační teorie a práva sehrál Viktor Knapp, který určil směr právní informatiky, který dodržují právníci dodnes. Knappovi se podařilo již v době prvních počítačů odhalit veliký potenciál informačních sítí. Díky nahlížení na právo jako na informační systém byl schopen publikovat unikátní vize budoucích aplikací. Ve svých prvních publikacích se občas hlásí k sovětské myšlence stroje na právo, přitom má skeptický pohled na tuto myšlenku.

Přestože sám Knapp upouští od svých předchozích vizí, objevují se ještě v půli osmdesátých let publikace, které připomínají využitelnost právních informačních technologií a informačních metod pro aktivní distribuci komunistické ideologie. Knapp se ve svých dalších publikacích zaměřuje více na instrumentální roli informačních technologií, přičemž se ve své poslední velké publikaci věnuje otázce aktivních rolí kybernetických metod při ideologizaci práva jen minimálně.

[1] POLČÁK R., Internet a proměny práva. [2012], strana 141

„V řadě otázek dokonce předvádí kopernikovský obrat, když opět s pozoruhodným instinktem naznačuje problémy nasazení informačních technologií. Na negativních příkladech nutně ukazujících na kapitalistické státy tak Knapp ilustruje byrokratizaci a odosobnění automatizovaných právních agend, problém ochrany osobních údajů nebo problémy kontroly justice exekutivou prostřednictvím kontroly justičních informačních systémů.“[1] Otázkami ochrany osobních údajů v informačních systémech, které nastínil Knapp v roce 1988, se začala právní věda zabývat až od poloviny devadesátých let.

V polovině sedmdesátých let se začínají objevovat na svou dobu výborné publikace, které rozebírají jednotlivé aspekty nasazení informačních technologií jako asistence právních procesů. Aplikace se přitom neomezuje jen na legislativu a justiční aplikace, ale i obchodní nebo obecně podnikové praxi. V polovině osmdesátých let je vytvořena nová právní disciplína – právo informačních a komunikačních technologií. Díky Knappovi byla Česká právní věda mezi prvními, které zachytily nástup této problematiky.

[1] POLČÁK R., Internet a proměny práva. [2012], strana 49

5. Proč autorizovat webový obsah

V dnešní době je spousta věcí dostupných přes webové aplikace. Je možné sledovat televizní pořady online, sledovat oblíbené pořady z archivu, číst jakékoli publikace online, atd. Z tohoto důvodu je dobré autorizovat webový obsah. Autorizovat webový obsah je výhodný prostředek jak na ochranu autorských práv, tak i na ochranu koncových uživatelů. V republice není trestné stahovat jakékoli soubory z internetu (až na určité výjimky jako je například dětská pornografie) na rozdíl od Německa či Velké Británie, kde je trestné i samotné stahování souborů, které jsou chráněny autorským zákonem. Nicméně v ČR je trestné dané věci šířit (sdílet na síti, umístit je na veřejný server).

Problematika autorských práv se nejvíce řeší u veřejných uložišť souborů, v ČR je velmi známý server ulozto.cz, na kterém se nachází spousta věcí, které jsou chráněny autorským právem, ale autor z nich ve většině případů neuvidí ani korunu. Podle evropského i českého práva nenesou provozovatelé těchto serverů odpovědnost za obsah, který tam uživatelé nahrávají. I když se na těchto server platí určité poplatky, aby se mohlo stahovat rychleji, tak tyto peníze zůstanou provozovateli a nikoli majiteli autorských práv stahovaných děl. Protože uživatel neplatí, aby si mohl stáhnout daný film, hru, program, ale platí si buď za vyšší přenosovou rychlost, popř. za větší objem dat. Policisté v dnešní době umí vystopovat počítač, ze kterého se nelegální kopie nahrávaly na server, ale pak nastane problém při dokazování, kdo počítač v době nahrávání souborů na server obsluhoval. Distributoři se nelegálnímu šíření brání najímáním lidí, kteří daná úložiště prohledávají a informují provozovatele uložiště o nelegálním obsahu. Ten je ze zákona povinen daný obsah odstranit z úložiště. Velcí distributoři, jako například Bonton film, tvrdí, že se jim v dnešní době nevyplatí vytvářet online videopůjčovny, protože by na šíření filmů po internetu museli nakoupit speciální práva a cenou pak nemohou konkurovat pirátským kopiím[1]. V případě autorizovaného webového obsahu, by to nebyl tak velký problém, kdyby se každý uživatel identifikoval například vlastním certifikátem (obdoba

[1] REPORTÉŘI ČT ze dne 26. 8. 2013, dostupné online: http://www.ceskatelevize.cz/porady/1142743803-reporteri-ct/213452801240033/video/

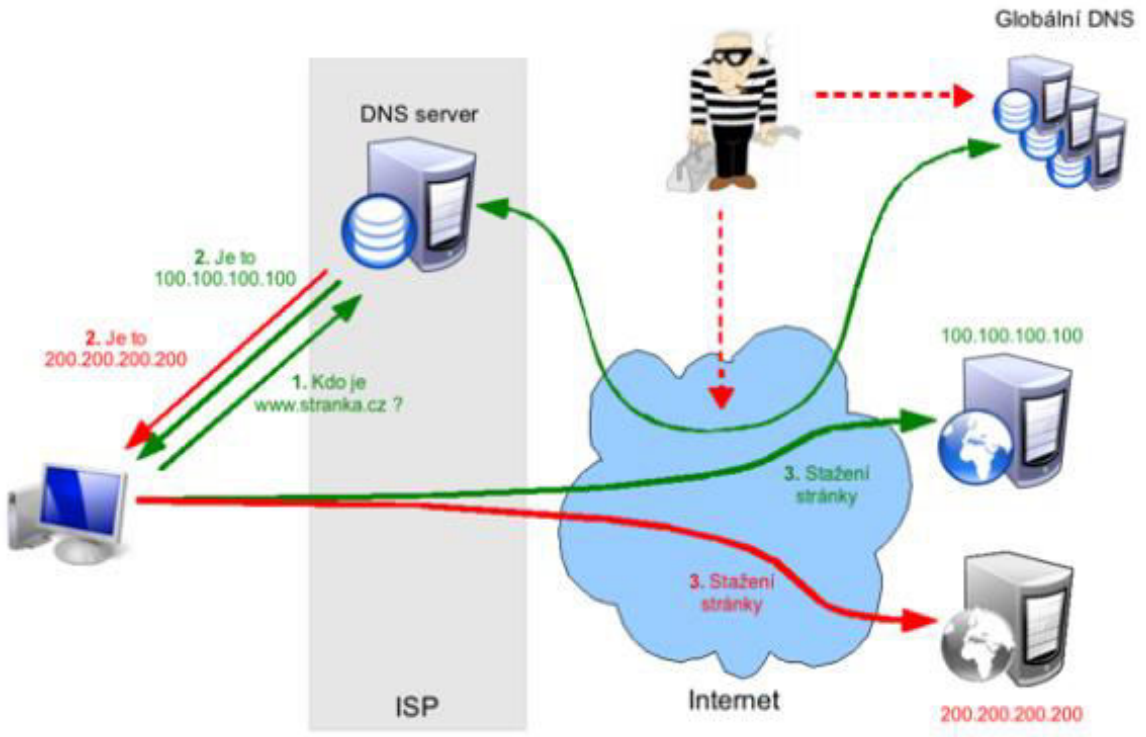
elektronického podpisu) popř. zakázáním nahrávání souborů na server nepřihlášeným (neidentifikovaným) uživatelům.

Ochrana koncového uživatele pomocí autorizace webového obsahu spíše spočívá v zajištění, že uživatel nebude nechtěně přesměrován na jiné stránky, kde může být nelegální obsah. Nebezpečí hrozí například při přesměrování na stránky, kde se nachází obsah s dětskou pornografií, protože konzumace dětské pornografie je ČR nelegální a uživatel by se mohl dostat do problémů. Toho by se dalo docílit několika způsoby, buď doménu chránit pomocí DNSSEC popř. vytvořit autorizační server, který by kontroloval požadavky a porovnával je s odpověďmi a kontroloval, jestli odpovědi nejsou nikterak pozměněné. Za jistou formu přesměrování se dá považovat i tzv. phishing (jedná se vytvoření podvodné stránky, e-mailu ve kterém se žádá, aby uživatel vyplnil citlivé údaje (hesla, čísla účtu, atd.). Jedinou obranou proti phishingu je nezveřejňování takovýchto citlivých údajů na internetu. Takovéto stránky případně e-maily se dají většinou poznat podle špatné češtiny, popř. odkazy směrují uživatele na špatné adresy.

5.1 DNSSEC

Protože služba DNS (domain name system) byla vyvinuta v době, kdy bylo k internetu připojeno malé množství lidí a počítačů, byla tato služba kompletně nezabezpečená. Když se internet stal veřejně přístupný, bylo nutné tuto službu nějakým způsobem zabezpečit, protože ne všichni uživatelé se připojují k síti se stejným úmyslem. Z tohoto důvodu byl vyvinut DNSSEC. DNSSEC je rozšíření služby DNS, které zvyšuje bezpečnost. Zajišťuje, že uživatel nedostal od DNS serveru podvržené údaje a informace byly poskytnuty správným zdrojem a nebylo s nimi nikterak manipulováno. Veškeré internetové služby (web, voip, iptv, e-mail, …) využívají DNS. Princip DNS je jednoduchý, jedná se o přeložení špatně pamatovatelné sekvence čísel (v případě IPv4) popř. hexadecimálních znaků (v případě IPv6) na srozumitelná slova. Například, když uživatel chce navštívit webovou stránku TUL, tak do prohlížeče napíše www.tul.cz, tuto adresu DNS server přeloží na ip adresu 147.230.16.27, která je zase srozumitelná pro počítače. Nebezpečí vzniká v případě, že je někdo schopný zasáhnout do komunikace a „podstrčit“ jinou

adresu, přičemž uživatel se vůbec nespojí se službou, kterou očekával. Situace je vyobrazena na obrázku č. 10.



Obrázek 10: Ilustrace principu DNS a útoku.
Zdroj: nic.cz, dostupné online: www.dnssec.cz

„Uživatel napíše do svého prohlížeče adresu, a za normálních okolností vše probíhá zeleně označenou cestou – použije server svého poskytovatele připojení ISP, a ten z globálního DNS získá číselnou adresu, se kterou se uživatel spojí a používá službu, kterou chtěl. V případě, že je však číselná adresa podvržena, pak vše probíhá červeně označenou cestou, a uživatel je spojen s jinou službou, aniž cokoli tuší.“[1]

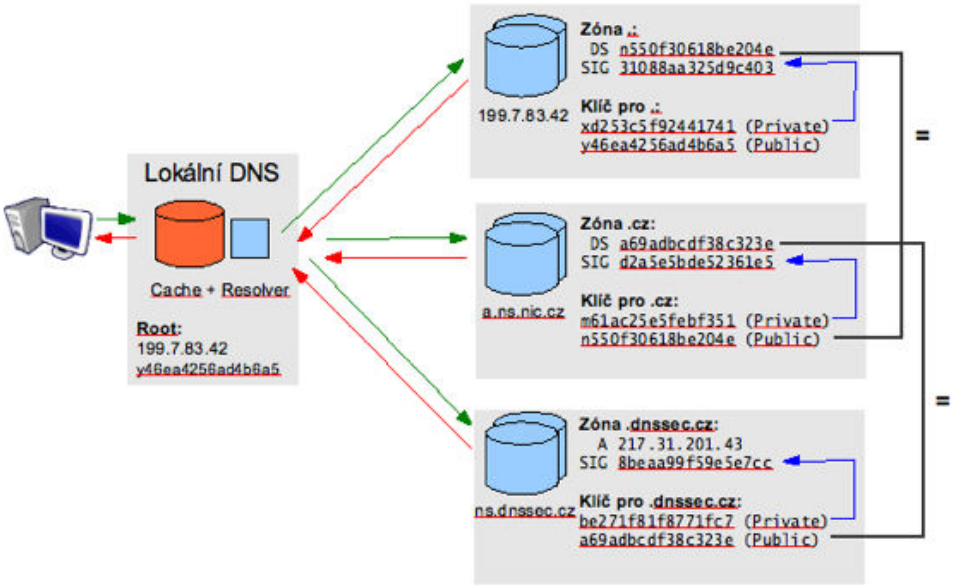
Podstrčení jiné adresy, může vypadat celkem neškodně, uživatel se například dostane pouze na jinou webovou stránku, než chtěl. Ale když půjde například o internetové bankovnictví, kam se zadávají přihlašovací údaje k bankovnímu účtu, tak z toho pak

[1] NIC.CZ, O DNSSEC, dostupné online: www.dnssec.cz

mohou být velké potíže. Stejně tomu tak bude, pokud bude uživatel odesílat e-mail s důležitými informacemi, v případě odvržené adresy si je pak může přečíst takřka kdokoli.

5.2 Princip fungování DNSSECu

Rozšíření DNSSEC zavádí asymetrickou kryptografii (jeden klíč na zašifrování údajů a druhý klíč na rozšifrování údajů). Jedná se o obdobu elektronického podpisu u elektronické komunikace. Pro využívání DNSSEC si majitel domény vygeneruje soukromý a veřejný klíč. Pomocí soukromého klíče digitálně podepíše informace o doméně v DNS, které se ověřují pomocí veřejného klíče. Z toho vyplývá, že veřejný klíč musí být dostupný pro všechny uživatele, z toho důvodu ho musí majitel umístit ke své doméně u nadřazené autority (pro .cz domény se jedná o registr domén .cz). Tímto způsobem se vytváří řetěz, který zajišťuje důvěryhodnost informací (vy případě že souhlasí elektronické podpisy), zobrazeno na obrázku 11.



Obrázek 11: Princip ověřování pomocí DNSSEC
Zdroj: nic.cz, dostupné online: http://www.dnssec.cz/page/444/jak-funguje-dnssec/

Koncový uživatel zavedení DNSSEC vůbec nepozná, protože DNSSEC je zpětně kompatibilní se systémem DNS a obě varianty fungují současně a to až do chvíle, kdy se na příslušném serveru začne používat DNSSEC (to může být firemní DNS server, DNS server od poskytovatele internetu, …). Poskytovatelům internetového připojení nasazení DNSSEC zvýší důvěryhodnost nabízených služeb, jen musí vytvořit digitální podpisy a publikovat je do registru domén.

5.3 Jak zavést DNSSEC

Zavádění rozšíření DNSSEC se liší podle typů uživatelů. Proces je různý, pokud je uživatel jen běžný koncový uživatel, a pokud se jedná například o ISP popř. majitele DNS serveru.

5.3.1 Zavedení DNSSEC z pohledu běžného uživatele

Uživatel musí vědět, jaký využívá DNS server (může mít vlastní DNS server, využívat DNS server od svého ISP) protože záleží na tom, kdo je správce DNS serveru, protože právě správce serveru musí zavést DNSSEC.

- Uživatel má vlastní DNS server
    - Zapnutí DNSSEC validace
    - Konfigurace bodu důvěry (nastavení klíče popř. otisku klíče, který je vrcholem důvěry pro ověřované záznamy)
- Uživatel využívá DNS server svého ISP
    - Zavedení rozšíření DNSSEC je záležitostí ISP.
    - Zjištění jestli ISP využívá DNSSEC je většinou možné z internetových stránek poskytovatele, dotazem na zákaznické zóně, popř. na stránkách www.dnssec.cz, kde je na pravé straně test využívání tohoto rozšíření.[1]
    - V případě, že ISP nevyužívá DNSSEC, je možné využít servery nic.cz, které jsou veřejně přístupné a využívají toto rozšíření.

[1] Zdroj: nic.cz, dostupné online: http://www.dnssec.cz/page/573/jak-zprovoznit-dnssec/

6. Konfigurace DNSSEC

Rozšíření DNSSEC je možné implementovat na jakémkoli DNS serveru, v současné době se hodně využívá DNS server Bind9, který je volně dostupný na linuxových distribucích (debian, ubuntu, …). Konfigurace samotného rozšíření je velmi jednoduché, jedná se o přidání pár řádků do konfiguračního souboru (named.conf):

```
options {
      . . .
      dnssec-enable: yes;
      dnssec-validation: yes;
      managed-keys-directory: „/cesta/ke/klicum/“
      . . .
}
```

Bod důvěry (veřejný klíč, který je nakonfigurován jako přístupový bod pro řetěz důvěry) je možné vytvořit dvěma způsoby, které se odvíjí od verze BINDu. Pro Bind 9.7 a novější verze stačí vložit do konfigurace následující text:

```
managed-keys {
"." initial-key 257 3 8 „AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcC
jFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq QxA+Uk1ihz0=";
};
```

Pro BIND 9.6 a starší je rozdíl pouze v začátku sekce, která vypadá takto:

```
trusted-keys {
 "." 257 3 8
```

Tato konfigurace zajistí automatickou aktualizaci klíče v případě, že bude klíč změněn dle RFC5011 - není nutný zásah do konfigurace systému. Na jiných serverech bude

konfigurace serveru téměř totožná, ne-li úplně identická. Klíč v příkladu je jen ukázkový správce si musí vygenerovat nový. Je také dobré se přihlásit do mailingové konference na nic.cz, kde jsou zveřejňovány technické informace týkající se .cz domény. Kvůli zabezpečení by se měl certifikát, kterým je podepsaná doména měnit každý měsíc (dle RFC), nevýhodou je, že jakákoli změna certifikátu může být zpoplatněna.[1]

[1] Zdroj: nic.cz, dostupné online: http://www.dnssec.cz/page/563/jak-zprovoznit-dnssec/

7. Rizika špatné autorizace

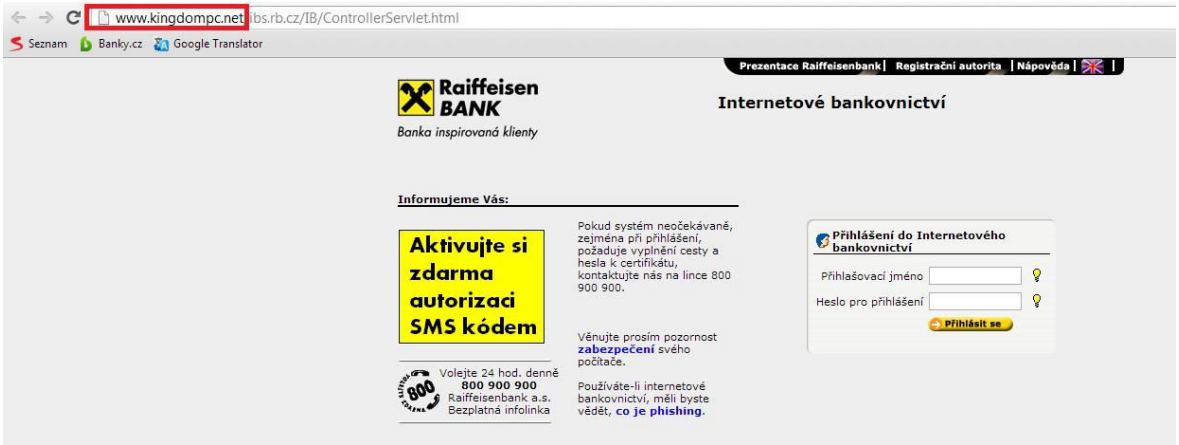
Díky špatné autorizaci případně díky špatnému DNS překladu mohou útočníci získat citlivé údaje (hesla do elektronického bankovnictví, přístupové údaje k e-mailům, čísla kreditních karet, atd.) jednotlivých uživatelů. Citlivé údaje se dají zajistit hned několika typy útoku, nejčastěji se jedná o phishing, pharming. Tyto typy útoků se dají ještě podpořit útokem na DNS server, který se nazývá DNS cache poisoning („otrávení vyrovnávací paměti DNS“).

7.1 Phishing

Phishing v podstatě není ani tolik útok jako spíše podvod, při kterém útočník (podvodník) získá citlivé údaje. Phishingové zprávy mají obvykle podobu falešných oznámení od bank, poskytovatelů, e-platebních systémů a dalších organizací. Zpráva se snaží donutit uživatele, aby z nějakého důvodu aktualizoval své osobní údaje. Častým důvodem uvedeným ve zprávě bývá chyba systému.[1]

Phishingové útoky jsou stále vyspělejší v jejich využití sociálního inženýrství. Ve většině případů se podvodníci snaží zastrašit příjemce zdánlivě důležitým důvodem, proč by měl uživatel vyplnit své údaje. Tyto zprávy obvykle obsahují hrozby zablokování účtu v případě, že nevyplní údaje zmíněné ve zprávě. Například: „Pokud nevyplníte své osobní údaje do konce týdne, váš účet bude zablokován“. Ironií je, že podvodníci často využívají jako důvod pro vyplnění osobních informací zlepšení anti-phishingového systému, například: „V případě, že se budete chtít zabezpečit proti phishingu, klikněte na odkaz níže a vyplňte přihlašovací údaje“.[1] Na obrázku 12 je zobrazena podvodná stránka (v tomto případě podvod na zákazníky raiffeisen bank), že je stránka podvodná, se dá zjistit podle adresy (červeně označeno).

[1] What is phising, dostupné online: https://www.securelist.com/en/threats/spam?chapter=85



Obrázek 12: Phishingová stránka
Zdroj: http://www.govcert.cz/cs/informacni-servis/zranitelnosti/phishing---stale-aktualni-hrozba/

Životnost phishingové stránky je v průměru 5 dní. Anti-phishingové filtry dostanou informaci o nové hrozbě velmi rychle a tak podvodníci musí neustále registrovat nové stránky, které imitují originální stránky různých organizací.[1]

Kvalita phishingové stránky je většinou velmi vysoká, podvodná stránka většinou vypadá úplně přesně jako originální, proto uživatel nebude mít žádná podezření, že je něco špatně a vloží své přihlašovací údaje[1], což může být například v případě elektronického bankovnictví velmi špatné.

Dalším phishingovým trikem je využívání adres, které vypadají podobně. Tento trik má polapit méně zkušené uživatele. Opatrný uživatel si všimne, že je adresa v prohlížeči něčím jiná od opravdové adresy. Tyto adresy mohou začínat IP adresou, i přesto, že velké společnosti takovéto adresy již nevyužívají. Adresy mohou využívat části správných adres, například místo www.rb.cz může být www.login-rb.cz.[1]

Úspěch phishingu je dán zejména nízkého povědomí uživatelů o tom, jak fungují společnosti, které se podvodníci snaží napodobit. Mnoho legitimních stránek obsahuje speciální varování, že nikdy nežádaly po uživatelích, aby odeslali důvěrná data. Nicméně uživatelé stále posílají svá hesla podvodníkům. Z tohoto důvodu byla před několika lety

[1] What is phising, dostupné online: https://www.securelist.com/en/threats/spam?chapter=85

založena Anti-Phishingová pracovní skupina (APWG - Anti-Phishing Working Group), která zahrnuje společnosti, které podvodníci napadli a společnosti, které vyvíjejí anti-phishingové/antispamové programy. APWG pořádá informační schůzky, aby informovaly uživatele o tomto problému. Kromě toho se členové APWG informují navzájem o nových phishingových stránkách a dalších hrozeb. V současné době má APWG kolem 2500 členů. Mezi nimi jsou velké mezinárodní banky a vedoucí IT firmy. Podle optimistické předpovědi budou uživatelé v brzké budoucnosti opatrní na phishingové stránky stejně jako na přílohy ve zprávách od neznámých zdrojů, jinak je jediná obrana dobrý spam filtr.[1]

Ochranou proti phishingu je spam filtr, ale ani ten v mnoha případech není úplně dostačující. Phishingové e-maily mají často chybnou gramatiku a slovosled, proto musí být uživatel obezřetný a všímat si těchto věcí, když něco takového uvidí a nebude to e-mail od někoho známého je lepší e-mail raději vyhodit a rozhodně neklikat na žádné odkazy a nevyplňovat nikde žádné důvěrné informace.

7.2 Pharming

Pharming je modernější a nebezpečnější nástupce phishíngu. Pharming využívá útoku na DNS, kde útočník pozmění příslušný záznam (změní IP adresu v daném záznamu), uživatel, který má využívá napadený DNS server, tak zadá správnou adresu, ale DNS ho odkáže na podvržený web, který vypadá stejně jako originální (stejně jako v případě phishingu). Jakmile uživatel vyplní přihlašovací údaje, tak je má útočník k dispozici.

Útočník nemusí nutně napadat DNS server, stačí mu pouze pozměnit hostovskou tabulku na počítači uživatele, to se dá udělat například pomocí trojského koně. Díky této změně nemusí ani zkušení uživatelé internetu přijít na to, že je stránka podvržená. Počítače uživatelů jsou také častěji napadány, protože povětšinou nemají takové zabezpečení jako DNS servery internetových poskytovatelů.

[1] What is phising, dostupné online: https://www.securelist.com/en/threats/spam?chapter=85

Na obrázku 13. je zobrazeno, jak může vypadat využívání napadeného DNS serveru, nebo počítače, kterému byla upravena hostovská tabulka. Uživatel chtěl jít na stránku adventuresinsecurity.com a místo toho se mu zobrazila stránka google.com. V případě, že by změna záznamu odkazovala na podvržené stránky například internetového bankovnictví, tak si změny všimne málo který uživatel.

Obrázek 13: Změna DNS záznamu
Zdroj: http://www.techrepublic.com/blog/it-security/hosts-file-pharming-and-other-botnet-recruiting-methods/

Jediná ochrana v případě pharmingu je jen dobrý a aktualizovaný antivirový program a používání důvěryhodných DNS serverů (většinou DNS server od poskytovatele internetu), popř. využít veřejný DNS server, který využívá rozšíření DNSSEC. Jedinou další možností jsou chyby na podvodné stránce (gramatika, slovosled, obrázky), ale to se často nestává, protože podvodné stránky jsou velmi propracované.

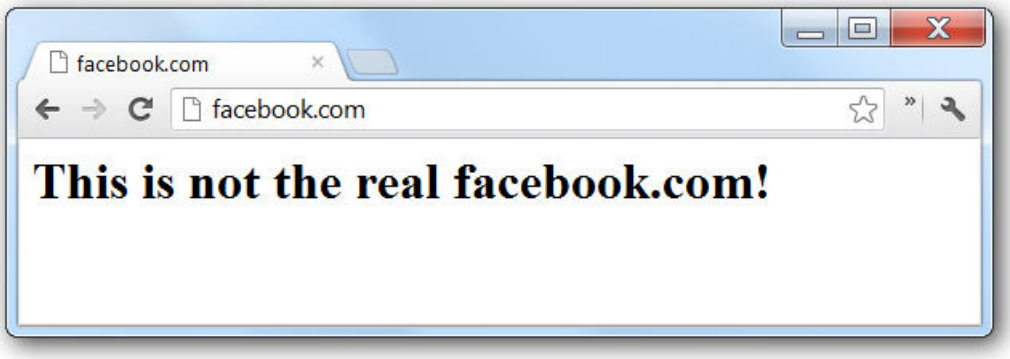
7.3 DNS cache poisoning

DNS cache poisoning je také znám pod pojmem DNS spoofing. Jedná se o útok, který využívá slabiny v DNS k odklonění toku dat od legitimních serverů k podvodným. Důvod proč je DNS cache poisoning tak nebezpečný je, že se může šířit z jednoho DNS serveru na další. Tento typ útoku způsobil, že čínský firewall dočasně opustil čínské hranice a cenzuroval internet v USA, dokud nebyl problém odstraněn.[1]

Internet nemá jen jeden DNS server, protože by to bylo velice neefektivní. Většina poskytovatelů internetu má vlastní DNS server, který ukládá informace od ostatních DNS serverů. Každý počítač má vlastní DNS cache, z důvodu, aby nemusel být při každém vyhledávání té samé adresy vysílán stejný požadavek na DNS server.[1]

DNS cache se stává „otrávenou“ v případě, že obsahuje nesprávné informace. Například, když útočník získá kontrolu nad DNS serverem a pozmění tam nějaké informace (útočník může pozměnit adresu například sociální sítě facebook a nasměrovat ji na vlastní adresu, která může být phishingová nebo pharmingová. Vyobrazeno na obrázku 14). Toto „otrávení“ se může šířit dál. Pokud uživatelův poskytovatel internetu dostává informace od „otráveného“ DNS serveru, tak se tato špatná informace (toto „otrávení“) rozšíří na DNS server poskytovatele, dále se může šířit do domácích routerů, případně do uživatelských počítačů.[1]

[1] What is DNS cache poisonint, dostupné online: http://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/



Obrázek 14: DNS cache poisoning
Zdroj: http://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/

Důvod proč je DNS cache poisoning taková hrozba je, protože není žádný způsob jak zjistit, jestli je odpověď z DNS serveru opravdová nebo podvržená. Dlouhodobé řešení je využívání DNSSECu. DNSSEC umožní podepsat jejich záznamy pomocí kryptografie s veřejným klíčem, který zajistí, že uživatelský počítač bude vědět, jestli má záznamu věřit, nebo jestli byly „otráveny“ a odkazují na jinou stránku.

8. Autorizace uživatelů na webových aplikacích

Způsobů jak autorizovat jednotlivé uživatele na portálech je mnoho. Každý se hodí pro různé webové aplikace. V prvé řadě je důležité si určit, jaká webová aplikace se bude provozovat, v případě některých aplikací je autorizace uživatelů zbytečná (např. webová prezentace firmy, restaurace, atd.), popř. je potřeba autorizovat uživatele jen v některých sekcích (komentáře, recenze, redakční zóna, atd.). Jiné webové aplikace naopak potřebují větší zabezpečení (administrační systémy firem, ve kterých jsou uchovávány citlivé data) a je potřeba autorizovat každého uživatele, aby se citlivá data nedostala do nesprávných rukou.

Možnosti autorizace uživatelů:

- Autorizace pomocí webserveru
- Autorizace pomocí Content Management Systém (CMS)
- Vlastní autorizace
- Vlastní autorizace s využitím frameworku

8.1 Autorizace pomocí webserveru

Konfigurace této autorizace se liší dle použitého webserveru. U velmi používaného webserveru apache je konfigurace poměrně jednoduchá, jsou dva způsoby jak autorizaci vytvořit. Webserver apache má dva typy autorizace[1], jedná se o:

- Basic
    - Základní http autentifikace uživatelů
    - Plná podpora prohlížečů
- Digest
    - Rozšířenější verze http autentifikace uživatelů
    - Nemá plnou podporu prohlížečů

[1] Dokumentace webserveru apache, dostupné online: http://httpd.apache.org/docs/2.2/howto/auth.html

Oba typy potřebují tzv. providera[1], ve kterém jsou uloženy přihlašovací údaje jednotlivých uživatelů. Provider může být:

- Anon
    - Pouze pro typ basic
    - Podobný způsob autentifikace jako u anonymního ftp. „Kouzelné“ uživatelské jméno anonymous a heslo e-mailová adresa, která se dá ukládat. Dá se kombinovat s dalšími přístupovými metodami (např. databáze) umožňuje efektivní sledování uživatelů včetně přístupu pro neregistrované uživatele.
- Dbd
    - Pro typ basic i digest
    - Pro autentifikaci využívá SQL databáze. Podobný způsob jako u providera File, akorát jsou uživatelé uloženi v tabulce v databázi místo v souboru.
    - Je potřeba nastavit mod_dbd, ve kterém se specifikuje nastavení databáze.
- Dbm
    - Pro typ basic i digest
    - Vyhledává uživatele v dbm souborech. Podobný jako provider File.
- File
    - Pro typ basic i digest
    - Autorizace uživatelů pomocí souborů s hesly bez jakéhokoli šifrování souborů
    - Soubory se vytvářejí pomocí utility htpasswd
- Ldap
    - Pro typ basic
    - Autorizace pomocí protokolu LDAP (lightweight directory access protokol)
    - Komplexní autorizace se dají implementovat pomocí LDAP filtrů
    - Podpora LDAP přes SSL
    - Využívá rozsáhlou cache LDAP operací pomocí módu mod_ldap

[1] Dokumentace webserveru apache, dostupné online: http://httpd.apache.org/docs/2.2/howto/auth.html

Jako poslední věc je potřeba nastavit, co je potřeba pro úspěšnou autorizaci, protože autorizace u webserveru (konkrétně apache) umožňuje zvyšovat granulitu například pomocí skupin uživatelů. To znamená, že se nemusí vyžadovat pouze validní uživatel, ale daný uživatel musí patřit do určité skupiny, aby se mohl přihlásit do dané aplikace. Takto autorizovaní uživatelé jsou autorizováni po celou dobu, po kterou mají otevřený prohlížeč.

8.1.1 Konfigurace serveru apache2

Webserver apache2 je možné konfigurovat dvěma způsoby. Buď v konfiguračním souboru dané webové aplikace, nebo pomocí konfiguračního souboru .htaccess (vhodné pokud je webová aplikace dostupná na více doménách). Pokud se bude autorizace konfigurovat pomocí souboru .htaccess je nutné, aby u virtual hostu měla volba AllowOverride hodnotu Auth, nebo all.

```
AuthType Basic
AuthName „Autorizace pomocí webserveru“
AuthUserFile /cesta/k/souboru/s/uživateli
AuthGroupFile /cesta/k/souboru/se/skupinami
Require group aplikace
```

Tento příklad rozděluje uživatele do skupin. Každý uživatel může být členem více skupin, toto rozdělení je vhodné zejména, když na webserveru běží více aplikací, ke kterým je potřeba kontrolovat přístup, protože díky tomuto řešení stačí pouze jeden soubor s uživateli a jeden soubor ve kterém jsou definováni členi jednotlivých skupin a nemusí být pro každou aplikaci zvláštní seznam uživatelů případně ještě definování skupin pro každou aplikaci.

Soubor s uživateli se spravuje pomocí příkazu htpasswd a má pevně určenou strukturu (uživatel:heslo), ve výchozím stavu je heslo lehce kryptováno, soubor se skupinou má také pevně danou strukturu (skupina: uživatel1 uživatel2), počet uživatelů ve skupině není omezen, je však potřeba, aby byly na jednom řádku.

8.1.2 Rizika při autorizaci pomocí webserveru

Při přetížení webserveru, popř. systému je možné, že webserver autorizuje uživatele i bez validních přihlašovacích údajů, popř. ani nebude vyžadovat autorizaci a zobrazí obsah aplikace. V případě provideru file, jsou hesla uložena v jednoduchém hashi v souboru, který může být dostupný uživatelům serveru, na kterém jede daná webová aplikace, je možné, že šikovný uživatel dokáže zjistit hesla, popř. soubory upravit, tak aby se do aplikace dostal. Stejný problém může nastat u provideru dbm, ale v tomto případě je již možný silnější hash na heslo, které by se nemělo dát tak snadno zjistit.

8.1.3 Eliminace rizik při autorizování pomocí webserveru

Pro eliminaci rizik je potřeba využívat webserver, který je stále podporován, aby se v případě problému vydala aktualizace, která daný problém vyřeší (ať už se jedná o memory leak, chyby v modulech, atp). Pokud se jedná o veřejný webserver, je potřeba bezpečnosti přizpůsobit celý systém souborů na serveru. Je dobré využívat chroot (který oddělí uživatele od sebe a od základního systému), takže si žádný uživatel nemůže prohlížet konfigurační soubory popř. je měnit, ale má maximálně přístup jen k jeho konfiguračním souborům (ale taky k nim nemusí mít přístup, záleží na konfiguraci, z hlediska bezpečnosti je lepší koncového uživatele omezit jak jen to je možné). Co se týká eliminace přetížení webserveru, tak jsou možnosti zvolit jiný (méně prostředkově náročný) operační systém (například místo windows serveru využít nějakou distribuci linuxu, které jsou zdarma i pro komerční využití a dají se tím ušetřit prostředky pro hardware serveru), popř. vylepšit hardware stávajícího serveru, což může být velmi finančně nákladné.

8.2 Autorizace pomocí CMS

U tohoto typu autorizace je velmi důležitá volba CMS. V případě, že se zvolí starý CMS, tak je velká pravděpodobnost, že se již v této době nevydávají žádné aktualizace a CMS může mít bezpečnostní díry, které by umožňovaly hackerům přístup k citlivým datům. Z tohoto důvodu je nutné vybírat mezi novými CMS, které se neustále vyvíjejí, a v případě bezpečnostního rizika vyjde aktualizace, která toto riziko eliminuje.

Mezi dobré CMS patří Drupal, WordPress, kteří jsou velmi modulární a dají se upravit, dle potřeby každého uživatele. Případně je možnost dopsání vlastních věcí, popř. jen upravit dle vlastní potřeby. V těchto systémech již je autorizace uživatelů předem naprogramována, a většinou využívá autorizaci pomocí SQL databáze. Autorizace na pomocí CMS systémů se dá kombinovat i s autorizací pomocí webserveru. Uživatel si většinou může nastavit, po jakou dobu zůstane uživatel přihlášen a vybrat, zda li chce využívat sessions popř. cookies pro kontrolu přihlášených uživatelů.

Rozdíl mezi sessions a cookies je v tom, že soubory cookie jsou ukládány do prohlížeče, který využívá uživatel a session ne. Tento rozdíl určuje jejich využívání. Cookie má v sobě uložené informace o uživateli (přihlašovací údaje) dokud není vymazaná – uživatel se nemusí neustále přihlašovat do systému (většinou dokud se neodhlásí). Nevýhoda je, že uživatel může soubory cookie blokovat popř. je kdykoli vymazat. Oproti tomu session se nadají vymazat, ale nemohou trvat tak dlouho jako cookie, protože jakmile se prohlížeč zavře, tak se veškeré údaje o session vymažou (v případě, že prohlížeč nevyužívá záložky a záložka nezůstane otevřená). Výhodou je, že session a cookies mohou spolu fungovat navzájem, takže se dá využít z obou to co je potřeba. Výběr CMS je omezen dle webserveru na kterém by CMS měl být spuštěn (zejména kvůli podpoře jazyku ve kterém byl CMS vytvořen), databáze na daném server (MS SQL, MySQL, Oracle), atd..

8.2.1 Rizika u CMS

Největší riziko nastává v případě, že se daný CMS nebude již aktualizovat. Takže v případě objevení bezpečnostního rizika je na uživateli, aby dané riziko eliminoval, což spousta uživatelů těchto CMS není schopná, protože využívají tyto CMS právě proto, že sami nejsou schopni takovéto věci naprogramovat. V tom případě je nutný přechod na jiný CMS, případně využít nějaký komerční CMS, u kterého se platí podpora a je zajištěna aktualizace v případě objevení bezpečnostního rizika.

8.2.2 Eliminiace rizik u CMS

Eliminace rizik v případě využití CMS je poměrně jednoduchá, stačí využívat moderní stále aktualizovaný systém. V případě, že bude uživatel chtít kvalitní CMS, který je v případě odhalení problému v podstatě ihned aktualizován a opětovně zabezpečen je nutné za takový systém zaplatit a to mnohdy nemalé peníze. Nekomerční a freewarové CMS často nejsou aktualizovány, a když jsou, tak ne stejnou rychlostí jako komerční a placené CMS.

8.3 Vlastní autorizace

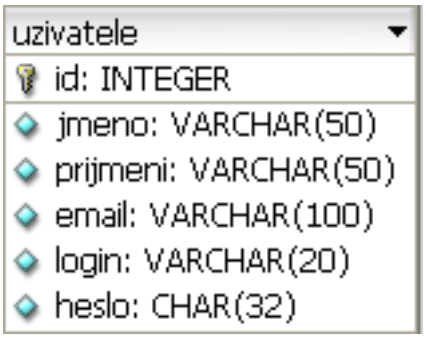
Touto autorizací se rozumí vývoj vlastní aplikace, ve které se budou spravovat uživatelé. Ještě před započetím programování je důležité se rozmyslet, jestli se budou využívat cookies, sessions nebo kombinace obou způsobů. Dále je potřeba se rozhodnout jestli bude určeno jedno heslo pro přístup (napsané v podmínce zdrojového kódu), nebo jestli bude systém více uživatelský případně, kde se budou uživatelé a jejich přihlašovací údaje skladovat (strukturovaný soubor, databáze). Nejjednodušší na správu uživatelů je databáze, kde se dají jednoduše dělat změny – upravení jednoho či více řádků v tabulce, vyhledávání. V případě uložení dat v souboru se už musí dodržovat předem daná struktura, v opačném případě to nebude nikdy fungovat, tak jak by mělo.

Z požadavků na práci s databází, sessionami popř. soubory cookie vyplývá, že je potřeba využít nějaký skriptovací jazyk, například PHP, ASP, Perl, atd.. U výběru skriptovacího jazyka závisí hodně na platformě serveru, webserveru a v neposlední řadě také na programátorovi, který bude systém vytvářet.

8.3.1 Návrh databáze

V případě, že by měl systém pracovat s databází (faktury, evidence zákazníků, …), je vhodné zvolit způsob autorizace s využitím databáze. Jedná se o vytvoření jedné (obr. 17, přihlášený uživatel má vše povoleno) popř. dvou tabulek navíc. Jedna tabulka na správu uživatelů, druhá na oprávnění, v případě, že by neměli mít všichni uživatelé stejný přístup.

K návrhu databáze je vhodné využít nějaký software, který umí vygenerovat SQL pro vytvoření tabulek včetně indexů na propojení mezi jednotlivými tabulkami (obr. 18).



Obrázek 15: Návrh tabulky pro správu uživatelů
Zdroj: vlastní tvorba

Obrázek 16: Návrh tabulek pro správu uživatelů a jejich oprávnění
Zdroj: vlastní tvorba

Na obrázku 15 je zobrazen návrh tabulky, ve které se budou uchovávat záznamy pouze o uživatelích. Návrh zobrazený na obrázku 16 je komplexnější, a umožňuje přidělovat uživatelům jednoduché oprávnění ve formě true nebo false – může nebo nemůže. Uživatelovo oprávnění se po úspěšném oprávnění může ukládat právě do session nebo do souboru cookie.

8.3.2 Přihlášení uživatele

Pro převzetí uživatelského vstupu se vytváří tzv. formuláře. Formulář pro přihlášení je velice jednoduchý, skládá se pouze ze dvou polí – uživatelské jméno (typ text) a heslo (typ

password, v podstatě stejný jako typ text, jen místo znaků zobrazuje tečky) a tlačítka na odeslání formuláře (typ submit). Formuláři se dále nastavuje metoda get nebo post. Metoda get je pro přihlašovací formulář nevhodná, protože se proměnné z formuláře zobrazují v adrese a žádný uživatel by nechtěl, aby jeho heslo mohl přečíst jakýkoli kolemjdoucí. Metoda post odesílá proměnné v hlavičce http požadavku – nejsou nikde vidět. K post proměnným se v jazyce PHP přistupuje pomocí proměnné $_POST – jedná se o indexované pole, kde index je vždy název pole ve formuláři (v ostatních jazycích to bude více méně stejné). Vlastní autorizace pak může v PHP vypadat například takto:

```
<?php
// spuštění sessions
session_start();
if( isset($_POST[‚login‘]) && isset($_POST[‚heslo‘]) ){
     // vložení skriptu na spojení s databází
     require(‚./db.php‘);
     $login = mysql_real_escape_string($_POST[‚login‘]);
     $heslo = md5($_POST[‚heslo‘]);
     $query = mysql_query(„SELECT id FROM uzivatele WHERE login LIKE ‚“ .
$login . “‘ AND heslo LIKE ‚“ . $heslo . “‘ “);
     if( mysql_num_rows($query) > 0) {
          // uživatel je veden v databázi -> uložení do session
          $_SESSION[‚uzivatel_id‘] = mysql_result($query, 0);
          // načtení oprávnění
          $_SESSION[‚opravneni‘] = (array)
mysql_fetch_object(mysql_query(„SELECT * FROM opravneni WHERE uzivatele_id = ‚“
. $_SESSIONS[‚uživatel_id‘] . “‘ LIMIT 1“));
     }
}
?>
```

Funkce mysql_real_escape_string() se využívá na ochranu před útočníky, kteří by chtěli pozměnit, popř. vymazat databázi se kterou systém pracuje. V návrhu se tato funkce používá pouze na přihlašovací jméno (login), na heslo není třeba, protože v návrhu databáze má heslo vyhrazené místo na přesně 32 znaků – hash md5 a zakodování hesla do md5 případným útokům zamezí. Tento způsob ukládání hesel je bezpečný, protože ani administrátor databáze nedokáže zjistit uživatelská hesla (prozatím se nepodařilo

rozšifrovat algoritmus md5). Po autentizaci uživatele může následovat například přesměrování na jinou stránku, kde už může uživatel pracovat se systémem. Každá stránka systému by pak měla začínat autorizací uživatele – práva uživatele jsou uložené v session, takže ani nemusí docházet ke komunikaci s databází. Autorizace uživatele:

```
<?php
// spuštění sessions
session_start();
// kontrola jestli má uživatel přístup
if( $_SESSION[‚opravneni‘]->modul == 1 ){
     // uživatel je autorizován využít tento modul
} else {
     // uživatel nemá povolení využívat tento modul -> přesměrování na úvod
     header(‚Location: index.php‘);
}
?>
```

Pro odhlášení uživatele v tomto případě pak stačí zavřít webový prohlížeč (pokud by byl systém otevřen v záložce, tak zavřít i záložku, jinak si prohlížeč bude nadále pamatovat informace o session), skript pro odhlášení by mohl vypadat takto:

```
<?php
session_unset();
header(‚Location: ./prihlaseni.php‘);
?>
```

Tento skript smaže veškeré údaje o session a následně přesměruje uživatele na stránku s přihlašovacím formulářem. Pokud se session ukládá do souboru, je lepší daný soubor smazat ze serveru funkcí unlink();

8.3.3 Rizika vlastní autorizace

Největším rizikem je nejspíše nezkušený programátor, který nemusí ošetřit všechny možnosti útoku (například SQL Injections, cross site scripting, brute force attack, …). V případě, že se hesla ukládají do databáze v prostém textu, existuje velké riziko, že daná

hesla někdo zneužije, zejména v případě, že uživatel používá stejné heslo k více věcem (e-mail, e-banking, atd.). Toto riziko platí zejména, zjistí-li nějaký útočník administrátorský přístup do databáze. Pokud programátor nebude moc ovládat jazyk SQL, může se stát, že díky špatně napsanému SQL dotazu na databázi bude autorizován uživatel, který ani není veden v databázi.

8.3.4 Eliminace rizik vlastní autorizace

V dnešní době je dostání spousta knih, ve kterých je detailně popsáno jak autentifikovat a následně autorizovat uživatele ve webové aplikaci, aby riziko špatné autorizace bylo minimalizováno pro jakýkoli skriptovací jazyk, kterým se dají takovéto aplikace vytvářet. Další možností je zajistit programátorovi nějaké školení, které se zabývá touto problematikou. Školení jsou výhodná zejména kvůli možnosti individuálního přístupu od školitele, naopak velkou nevýhodou je cena školení. Ceny těchto školení se pohybují v řádech desetitisíců. Je také důležité nikam (databáze, strukturovaný soubor) neukládat hesla v prostém textu. Hesla je výhodné ukládat v hashi, který útočníkovi zamezí zjištění hesla v případě, že se dostane k přihlašovacím údajům (ať už jsou v databázi nebo ve strukturovaném souboru). Velmi často využívané hashe jsou md5 a sha1, malý problém je, že na tyto hashe již existují slovníky, ale tomuto nebezpečí se dá předcházet v případě kombinace obou hashů. Existují i jiné hashe, je ale potřeba se podívat jestli jsou bezpečné, a nedají se snadno prolomit. Eliminace nízké znalosti jazyka SQL pro komunikaci s databází se dá předejít knížkou, kde je jazyk SQL vysvětlen, školením na databázové systémy případně místo databáze využít strukturovaný soubor pro ukládání uživatelů.

8.4 Vlastní autorizace s využitím frameworku

Framework přebírá typické problémy dané oblasti, díky tomu je vývoj usnadněn, protože se vývojáři mohou soustředit pouze na své zadání. Vývojář díky frameworku například nemusí řešit navigaci mezi stránkami, protože to za něj udělá framework. Frameworky také často využívají návrhový vzor MVC (obrázek 19), který odděluje programovou část od zobrazovací části a kód je pak přehlednější. V případě, že je framework psán objektově, tak se skládá z abstraktních tříd, které může vývojář využít k vytvoření vlastních tříd dle

potřeb daného projektu. Další výhodou frameworků, je testování napsaných kódů pomocí tzv. unit testů, které jsou schopny zobrazit nevyužitý kód, kontrolovat oprávnění atd. Mezi velmi často využívané frameworky patří Zend Framework (ZF), který je objektově orientovaný a vyvíjen s ohledem na jednoduchý vývoj aplikací. ZF obsahuje komponenty pro MVC aplikace, autorizaci a autentifikaci, různé druhy cache, různé filtry a validátory.

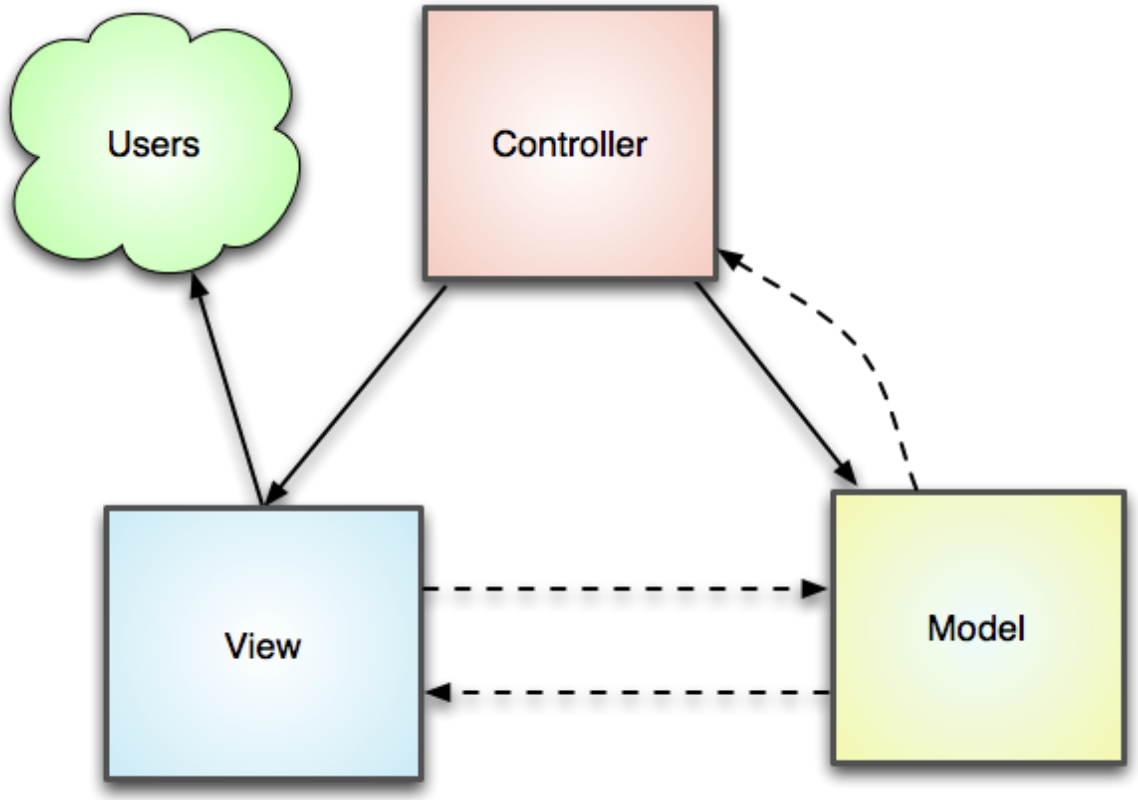
Vlastnosti ZF:

- Veškeré komponenty jsou objektově orientované
- Modulární architektura
- Implementuje MVC
- Podpora multidatabázových systémů

8.4.1 Návrhový vzor MVC

MVC je standard pro design moderních webových aplikací. Většina kódu webové aplikace spadá do jedné ze tří kategorií – prezentační, programátorská logika (obchodní logika), přístup k datům. MVC modely tyto kategorie od sebe navzájem oddělují. Díky tomu může být kód pro prezentaci v jedné části aplikace, programátorská logika v druhé části a přístup k datům v jiné části. Mnoho vývojářů považuje toto oddělení jednotlivých částí od sebe nezbytných k udržování a organizování kódu aplikace, zvláště v případě, že se na vývoji aplikace podílí víc než jeden vývojář[1].

[1] Dokumentace Zend Frameworku, dostupné online:
http://framework.zend.com/manual/1.12/en/learning.quickstart.intro.html



Obrázek 17: Způsob fungování MVC aplikace
Zdroj: http://framework.zend.com/manual/1.12/en/learning.quickstart.intro.html

- **Model** – V této části se definuje základní funkčnost aplikace a vytvářejí se abstrakční třídy. Může zde být také definován přístup k datům (databáze, strukturované soubory, atd.) a programátorská logika[1]
- **View –** View (pohled) definuje přesně, co je prezentováno uživateli. Obvykle předává controller data do pohledu, který je vykreslí v nějakém formátu. Pohledy také přebírají data od uživatele. V této části se nachází (X)HTML. [1]
- **Controller** – Controller (dispečer) spojuje všechny části dohromady. Pracují s modely, určují, který pohled se bude zobrazovat podle uživatelských požadavků a dalších faktorů, předávají data, které potřebuje pohled, popřípadě předají kontrolu jinému dispečeru. Doporučuje se mít dispečery co nejjednodušší.[1]

[1] Dokumentace Zend Frameworku, dostupné online:
http://framework.zend.com/manual/1.12/en/learning.quickstart.intro.html

8.4.2 Přihlášení uživatele s využitím ZF

ZF ulehčuje vytváření formulářů a přidává k nim filtrování vstupních dat, a validování dat. Filtry umožňují odstranění dat, které nejsou žádané (zamezení útokům jako jsou SQL injections). Validace údajů se hodí v případě robotů nebo brutálních útoků (brute force attack) – v případě nevalidních údajů nebude docházet ke zbytečné komunikaci s databází. Formulář může být nadefinován takto:

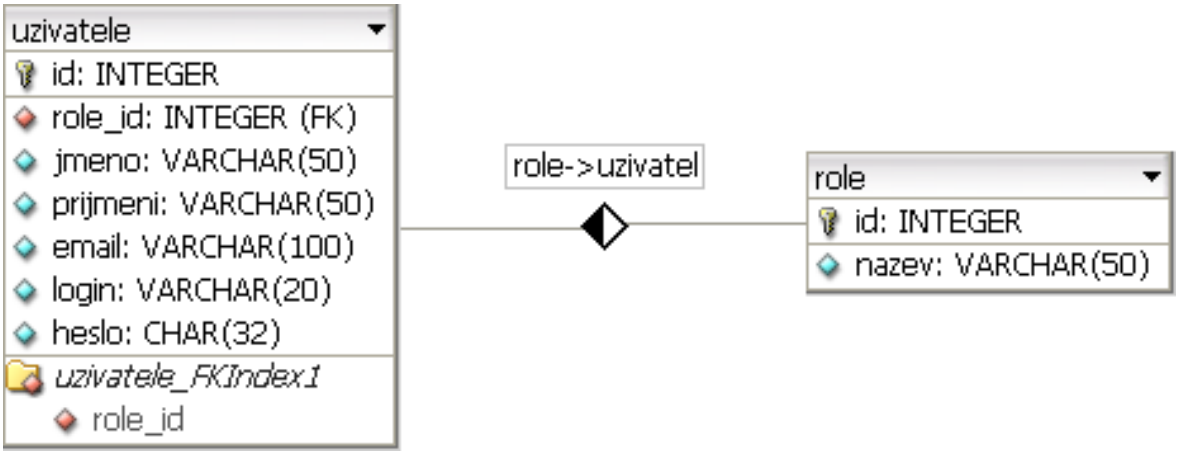
```
<?php
class Form_Prihlaseni extends Zend_Form {

	/*
	 * definování formuláře
	 */
	public function init(){
		// akce
		$this->setAction('/prihlaseni/');
		// metoda
		$this->setMethod(Zend_Form::METHOD_POST);
		// ID formuláře
		$this->setAttrib('id', 'login');

		// uživatelské jméno
		$jmeno = new Zend_Form_Element_Text('jmeno', array(
			'label' => 'Uživatelské jméno',
			'required' => true
		));
		// pouze alfanumerické znaky
		$jmeno->addFilter(‚Alnum‘);
		// heslo
		$heslo = new Zend_Form_Element_Password('heslo',array(
			'label' => 'Heslo',
			'required' => true
		));
		$heslo->addFilter(‚Alnum‘);
		// validátor na heslo – musí mít alespoň jedno číslo, nebo písmeno,
a jedno písmena musí být odlišnou velikostí
		$heslo->addValidator(‚Regex‘, false, '/^(?=.*\d)(?=.*[a-z])(?=.*[A-
Z])(.){8,}$/');
		// submit element
		$submit = new Zend_Form_Element_Submit('prihlaseni', array(
			'value' => 'Přihlásit'
		));
		// přidání polí do formuláře
		$this->addElements(array($jmeno, $heslo, $submit));
	}
}
```

Samotná autorizace a autentizace se dá v ZF vytvořit pomocí pluginu pro dispečer. V tomto pluginu se budou zejména využívat komponenty Zend_Auth – pro autentizaci

uživatele a Zend_Acl pro autorizaci uživatele. Výhoda využívaní autentizace a autorizace v pluginu pro dispečer je, že se automaticky provádí kontrola při každém načtení stránky a programátor, tak na to nemusí neustále myslet a psát kontrolu do každého skriptu, který bude programovat do systému. Metoda na přihlášení a odhlášení:

```
protected function _prihlas(Zend_Controller_Request_Abstract $request){
	// údaje z post pole
	$post = $request->getPost();
	$odhlas = $request->getParam('odhlasit');
	// zjištění jestli se vůbec přihlašovalo
	if( isset($post['prihlaseni']) ){
		// získání databázového controlleru
		$frontController = Zend_Controller_Front::getInstance();
		$bootstrap = $frontController->getParam('bootstrap');
		$resource = $bootstrap->getPluginResource('multidb');
		$db = $resource->getDb('server');
		// filtrování údajů
		$login = Zend_Filter::filterStatic($post['jmeno'], 'Alnum');
		$heslo = Zend_Filter::filterStatic($post['heslo'], 'Alnum');
		// adaptér na přihlášení
		$authAdapter = new Zend_Auth_Adapter_DbTable($db,
'webmin_uzivatele', 'login', 'heslo', 'MD5(SHA1(?))');
		// nastavení přihlašovacích údajů
		$authAdapter->setIdentity($login);
		$authAdapter->setCredential($heslo);
		// pokus o autentizaci
		if( !Zend_Auth::getInstance()->authenticate($authAdapter)-
>isValid() ){
			// nepodařilo se autentizovat
			Zend_Auth::getInstance()->getStorage()->clear();
			Zend_Auth::getInstance()->clearIdentity();
			Zend_Session::destroy();
			Zend_Session_Namespace::resetSingleInstance('Zend_Auth');
		} else {
			// podařilo se autentizovat
			$identita = $authAdapter->getResultRowObject(null, 'heslo');
			$roleId = ($identita->role_id == '') ? 1 : $identita-
>role_id;
			$identita->role = $db->fetchOne($db->select()-
>from('webmin_role', 'role')->where('id = ?', $roleId)->limit(1));
			Zend_Auth::getInstance()->getStorage()->write($identita);
		}
	} elseif( $odhlas == "true" ){
		Zend_Auth::getInstance()->getStorage()->clear();
		Zend_Auth::getInstance()->clearIdentity();
		Zend_Session::forgetMe();
		Zend_Session::destroy();
		Zend_Session_Namespace::resetSingleInstance('Zend_Auth');
	} else {
		if( !Zend_Auth::getInstance() ){
			Zend_Session::forgetMe();
		}
	}
}
```

Autorizace u ZF provádí komponenta Zend_Auth. Každý uživatel má přiřazenou roli a každá role má přiřazené oprávnění (to je výhodné při přiřazování stejného oprávnění více uživatelům, přiřadí se pouze role a není nutné nastavovat každému uživateli zvlášť oprávnění pro každý modul, další výhodou je možnost dědění oprávnění). Kvůli tomuto způsobu nastavování oprávnění je nutné navrhnout databázi trochu jinak (obrázek 18). Tento princip jde využít i u vlastní autorizace, nicméně aplikace nebude tak jednoduchá jako u příkladu, který je uveden.



Obrázek 18: Úprava databáze pro přiřazování rolí
Zdroj: vlastní tvorba

Aby autorizace probíhala správně, musí se nadefinovat role a tzv. zdroje, jakmile jsou tyto věci nadefinované, je nutné nadefinovat oprávnění pro každou roli na každý zdroj, výchozí politika je „co není povoleno, je zakázáno“:

```
// definování rolí
$this->addRole(new Zend_Acl_Role('host'));
// role uživatel dědí práva od role host
$this->addRole(new Zend_Acl_Role('uzivatel'), 'host');
//  role administrátor dědí oprávnění od role uzivatel
$this->addRole(new Zend_Acl_Role('administrator'), 'webmaster');
// definování zdrojů
$this->addResource(new Zend_Acl_Resource('index'));// přihlášení
$this->addResource(new Zend_Acl_Resource('modul1'));// Modul 1
$this->addResource(new Zend_Acl_Resource('modul2'));// Modul 2
$this->addResource(new Zend_Acl_Resource('modul3'));// Modul 3
$this->addResource(new Zend_Acl_Resource('modul4'));// Modul 4
$this->addResource(new Zend_Acl_Resource('error'));// Zobrazování chyb
// definování přístupů
$this->allow('host', 'index');
$this->allow('host', 'error');
$this->allow('uzivatel', 'modul1');
```

```
$this->allow('uzivatel', 'modul2');
$this->allow('administrator', 'modul3');
$this->allow('administrator', 'modul4');
```

Autorizace v pluginu pro dispečer probíhá pouze pomocí volání metody „isAllowed()“, která vrací hodnoty true nebo false (přístup povolen nebo přístup zakázán). Autorizace se provádí před odesláním stránky pro uživatele (kdyby uživatel neměl patřičná oprávnění, je nutné, aby se vykreslila jiná stránka, než uživateli, který patřičná oprávnění má):

```
public function dispatchLoopStartup(Zend_Controller_Request_Abstract $request){
	// přihlásíme se
	$this->_prihlas($request);
	// pokud je uživatel přihlášen tak mu přiřadíme jeho roli pokud ne, tak 
přiřadíme roli host
	$role = Zend_Auth::getInstance()->hasIdentity() ? 
Zend_Auth::getInstance()->getIdentity()->role : 'host';
	// získání instance ACL
	$acl = Acl::getInstance();
	// kontrola jestli má uživatel přístup
	if( !$acl->isAllowed($role, $request->getControllerName(), $request-
>getActionName()) ){
		// nemá práva k přístupu
		$novaAkce = ( $role == 'host' ) ? '' : 'zakazano';// pokud je 
přihlášen vypíše se "přístup odepřen" jinak se přesměruje na přihlášení
		$novyController = ( $role == 'host' ) ? '' : 'error';
		$request->setModuleName('default');
		$request->setControllerName($novyController);
		$request->setActionName($novaAkce);
	}
}
```

8.4.3 Rizika vlastní autorizace s využitím frameworku

Díky využívání již předepsaných autorizačních a autentifikačních funkcí je riziko špatné autentifikace nebo úspěšného útoku menší než u vlastní autorizace. Riziko vzniká v případě, že framework bude využívat nezkušený programátor, který nebude tyto předepsané komponenty využívat, popřípadě je bude využívat špatně. V případě využívání méně známých frameworků, nebo dlouho neaktualizovaných frameworků mohou být chyby nebo bezpečností díry přímo v předepsaných komponentech.

8.4.4 Eliminace rizik vlastní autorizace s využitím frameworku

Pokud se bude framework využívat, způsobem jakým byl navržen, jsou rizika sami o sobě minimální. To se dá zajistit knihou, ve které je vysvětleno jak daný framework správně využívat, popřípadě jít na školení. Školení je výhodné zejména v případě, že programátor musí řešit nějaký unikátní problém, na který nemůže najít vhodné řešení ani v knížce ani v dokumentaci k danému frameworku, nicméně je stále potřeba využívat aktuální framework, u kterého se případné bezpečnostní problémy budou řešit zkušenými vývojáři.

Závěr

V diplomové práci jsem řešil autorizaci webového obsahu a to jak z hlediska zobrazení správné webové stránky, tak i autorizaci uživatelů webových aplikací. Pro tuto práci bylo nejprve nutné seznámit se s právem na internetu, aby bylo odůvodněné, proč je důležité autorizovat webový obsah. Dále bylo nutné seznámit se s principem fungování překladu doménových jmen na adresy (DNS) a jeho možnosti rozšíření. Poté bylo možné analyzovat možná rizika a hledat na ně vhodná řešení. Pro autorizaci uživatelů webových aplikacích bylo nutné nejprve zjistit, jaké jsou možnosti autorizování uživatelů ve webových aplikacích. Podle průzkumu na internetu jsem vybral nejpoužívanější metody autorizace uživatelů a hledal jejich možná bezpečnostní rizika a následně možné řešení daných bezpečnostních rizik.

Zobrazení požadované stránky se dá zajistit poměrně lehce využitím bezpečnostního rozšíření DNSSEC v systému DNS. Toto rozšíření bohužel nemohou lehce sprovoznit na svých stanicích koncoví uživatelé. Rozšíření DNSSEC musí zapnout majitel DNS serveru respektive poskytovatel internetových služeb. V případě, že poskytovatel nebo majitel DNS serveru nevyužívá rozšíření DNSSEC a uživatelé mají možnost nastavit si vlastní DNS, mají možnost nastavit si veřejně dostupné DNS servery, které toto rozšíření využívají. Nicméně si tím mohou omezit přístup na servery ve vnitřní síti svého poskytovatele. Konfigurace tohoto rozšíření není komplikovaná a je popsána v kapitole 6. Rizika špatné autorizace resp. přesměrování na podvodné stránky jsou popsány v kapitole 7. Implementace DNSSEC není vždy úplně bezproblémová, zejména kvůli finanční stránce. Výměna klíčů každý měsíc (dle pravidel RFC) může být velice nákladná, proto není DNSSEC moc využívaný nástroj. Právě z toho důvodu se nabízí rozpracování dalších možností kontroly správného zobrazení webového obsahu, které však byly mimo rozsah této práce.

Protože doposud nebyl napsán ani vymyšlen nějaký standard pro autorizaci webového obsahu, často se pojem autorizace spojuje s termínem autentifikace uživatelů. Jakmile je uživatel ověřen (autentifikován), je možné přikročit k jeho autorizaci (nastavit práva v systému). Právě tímto problémem jsem se zabýval v kapitole 7, kde jsem využil i své zkušenosti z firem Miton.cz, Metronet a občanského sdružení mh2net.

Analýzou dostupných zdrojů jsem zjistil, že mezi nejčastěji využívané autorizace uživatelů pomocí webserveru, různých CMS systému nebo individuálně vyvíjeným systémem. Autorizace pomocí webserveru je poměrně jednoduše nastavitelná a celkově jednoduchá, nicméně velké komplikace nastávají při autorizování širších komplexnějších systémů. V případě rozsáhlého systému (například STAG) je tato autorizace více méně nepoužitelná.

Autorizace uživatelů s využitím CMS systémů se zejména využívá v případě redakčních systémů, kde je většina obsahu veřejně přístupného, jen do administrátorské sekce jsou autorizováni pouze někteří uživatelé. Z toho plyne, že tento typ autorizace je vhodný na různé blogy, webové prezentace firem a podobné typy stránek. Co se týká bezpečnosti při autorizaci uživatelů, tak záleží zejména na volbě daného CMS systému, jak je popsáno v kapitole 8.2.

Vývoj individuálního systému podle svých zkušeností z výše zmíněných firem jsem rozdělil na dvě části, čistě vlastní autorizace a vlastní autorizace s využitím frameworku. Toto rozdělení jsem udělal zejména, aby bylo ukázáno, jak dokáže framework autentifikaci a následnou autorizaci zjednodušit a více zabezpečit oproti ryze vlastní vyvíjené autentifikaci a autorizaci. Dalším důvodem bylo, že ne každý programátor, který vyvíjí webové systémy, nepoužívá (případně neumí používat) frameworky. V obou případech velice záleží na zkušenostech programátora, který systém vyvíjí, jakmile nemá dostatek zkušeností, je nezbytné, aby využil nějakou literaturu zaměřenou na toto téma, jinak hrozí nebezpečí chybné autorizace (v tomto případě je jedno, jestli využívá nebo nevyužívá framework).

Po analýze uvedených typů autorizace je patrné, že každý druh autorizace má své výhody a nevýhody. Bohužel na ani jeden z nich se nedá spolehnout na 100%, nicméně je možné se této jistotě přiblížit například kombinací jednotlivých druhů autorizace uživatelů. Ještě vyššího stupně zabezpečení by se dalo ještě dosáhnout využitím například virtuální privátní sítě (VPN) a webserver na kterém je webová aplikace nakonfigurovat, tak, že by se na aplikaci dalo dostat pouze z adresního prostoru VPN. Další možností rozšíření zabezpečení by mohlo například být posílání SMS správ na telefon, který mají uživatelé uvedený u svého účtu s autorizačním kódem. Bohužel takováto bezpečnostní rozšíření jsou

velmi nákladné, a ne každý si je může dovolit, nicméně se správnou konfigurací webového serveru a dobře napsanou aplikací (ať už CMS nebo vlastní vývoj) se dá vytvořit dostatečně bezpečné řešení autorizace uživatelů.

Cíle této práce byly splněny, pomocí bezpečnostního rozšíření DNSSEC pro systémy DNS, které zajistí bezpečné procházení internetu. Pro autorizaci uživatelů webových aplikací byly navrženy skripty v kapitole 8.2 a 8.3, které byly prakticky ověřeny.

Seznam použité literatury

POLČÁK R., *Internet a proměny práva.* 1. Vyd. Praha: Auditorium, 2012. 388 s. ISBN 978-80-87284-22-3

BÖHMER M., *Zend Framework Programujeme webové aplikace v PHP*, Computer press, 2010, 416 s., ISBN 978-80-251-2965-4

INDRAKANTI, S., VARADHARAJAN, V. and HITCHENS, M., Authorization Service for Web Services and its Application in a Health Care Domain. *International Journal of Web Services Research*, 2005, strana 94-119 ProQuest Central; ProQuest Technology Collection. ISSN 15457362.

INTERNET SOCIETY, Internet Society Collaborates with Shinkuro and Parsons to Promote Global Deployment of Domain Name System Security Extensions DNSSEC. *Bioterrorism Week*, 2013, strana 10 ProQuest Central; ProQuest Hospital Collection; ProQuest Natural Science Collection. ISSN 15478602.

BELLOVIN S., *Using the DNS for System Break-Ins,* Proc. Usenix, Security Symp., 1995

YANG, H., et al., *Deploying Cryptography in Internet-Scale Systems: A Case Study on DNSSEC. IEEE Transactions on Dependable and Secure Computing*, 2011, strana 656-669 ProQuest Central; ProQuest Technology Collection. ISSN 15455971. Dostupné online: http://dx.doi.org/10.1109/TDSC.2010.10.

MARSAN, C.D., Domain Vendors Tackle DNS Security. *Network World*, 2008, strana 10, ProQuest Central; ProQuest Technology Collection. ISSN 8877661.

ARENDS R., AUSTEIN R., LARSON M., MASSEY M., a ROSE S., *DNS Security Introduction and Requirement*, RFC 4033, 2005

ARENDS R., AUSTEIN R., LARSON M., MASSEY M., a ROSE S., *Protocol Modifications for the DNS Security Extensions*, RFC 4035, Mar. 2005.

ARENDS R., AUSTEIN R., LARSON M., MASSEY M., a ROSE S., *Resource Records for the DNS Security Extensions*, RFC 4034, 2005.

KENT S. a ATKINSON R., *security Architecture for the internet Protokol*, IETF Network Working Group RFC 2401, 1998, dostupné online: http://www.ietf. org/rfc/rfcl825.txt.

KENT S. a ATKINSON R., *IP Authentication Header*, IETF Network Working Group RFC 2402, 1998.

KENT S. a ATKINSON R., *IP Encapsulating security Payload*, IETF Network Working Group RFC 2406, 1998

GUTTMAN J. D.,HERZOG A. L.,a THAYER F. J., *Authentication and Confidentiality via IPsec*, Proceedings of the Sixth European Symposium on Research in Computer security - ESORICS 2000, Lecture Notes in Computer Science 1895, 2000, dostupné online: http://www.ccs.neu.edu/home/ gullman/esoricsipsec.pdi.

PERLMAN R. a KAUFMAN C., *Analysis of the IPSec Key Exchange Standard*, Proceedings of the Tenth IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative EnterprisesWET ICE 2001, dostupné online: http://sec.fenito.org/wetice-2001/papers/ radia-paper.pdf, 2001.

SHINDER D., *securing Data in Transit with IPsec*, 2003, dostupné online: http://www.windowsecurity.com/articles/Securing_Data_in_Transit_with _IPSec. html.

WU C.-L., WU S. F., a NARAYAN R., *IPSec/PHIL (Packet Header Information List): Design, Implementation, and Evaluation*, Proceedings of the Tenth International Conference on Computer Communications and Networks, 2001, dostupné online: http://www.cs.ucdavis.edu/~wu/publications/ 314-PHIL.pdf.

THOMAS, J. a ELBIRT, A.J., *Understanding Internet Protocol Security. Information Systems Security*, Sep, 2004, strana 39-43 ProQuest Central; ProQuest Hospital Collection; ProQuest Technology Collection. ISSN 1065898X.

HARRIS TECHNOLOGY, Llc, *Patent Application Titled "using Biometrics as an Encryption Key"* Computers, Networks & Communications, 2013. strana 731 ProQuest Central; ProQuest Science Journals; ProQuest Technology Collection.

ZHANG, Y.L. a XIA, *G.S., The SSL MIMT Attack with DNS Spoofing. Applied Mechanics and Materials*, 2013, strana 1647 ProQuest Technology Collection. ISSN 16609336. Dostupné online: http://dx.doi.org/10.4028/www.scientific.net/AMM.385-386.1647.

EMC CORPORATION, *Patent Issued for System and Method for Detecting and Mitigating DNS Spoofing Trojans*. Computers, Networks & Communications, strana 2493 ProQuest Central; ProQuest Science Journals; ProQuest Technology Collection.

JAMES L., *Phishing exposed. Tech target article sponsored by: Sunbelt software*, 2006, dostupné online: searchexchange.com.

PURKAIT, S., *Phishing Counter Measures and their Effectiveness* - Literature Review. Information Management & Computer Security, 2012, strana 382-420 ProQuest Central; ProQuest Hospital Collection; ProQuest Technology Collection. ISSN 09685227. Dostupné online: http://dx.doi.org/10.1108/09685221211286548.

EMM D., *Phishing update, and how to avoid getting hooked*, 2006, strana 13-15.

SHENG S., MAGNIEN B., KUMARAGURU P., ACQUISTI A., CRANOR L., HONG J. a NUNGE E., *Antiphishing phil: the design and evaluation of a game that teaches people not to fall for phish*, SOUPS'07: Proceedings of the 3rd Symposium on Usable Privacy and Security, 2007, New York, NY, strana 8899.

HINDE S., *All you need to be a phisherman is patience and a worm*, Computer Fraud & Security, 2004, strana 4-6.

MERCURI R.T., *Scoping identity theft*, Communications of the ACM, 2006, strana 17-21.

EISTEIN E.M., *Identity theft: an exploratory study with implications for marketers*, Journal of Business Research, 2008, strana 1160-72.

BRODY R.G., MULIG E. a KIMBALL V., *Phishing, pharming and identity theft*, Academy of Accounting and Financial Studies Journal, 2007, strana 43-56.

ANDERSON K.B., DURBIN E. a SALINGER M.A., *Identity theft*, Journal of Economic Perspectives, 2008, strana 171-92.

CASTILLO M.D., IGLESIAS A. a SERRANO J.I., *Detecting phishing e-mails by heterogeneous classification*, in Yin, H. et al. (Eds), 2007, strana 296-305.

KNIGHT, W., *Caught in the net*, IEEE Review, 2005, strana 26-30.

MURPHY J.M., *The water is wide: network security at Kenyon College,* Proceedings of the 33rd Annual ACM Conference on User Services, SIGUCCS 2005, Monterey, CA, USA, strana 237-40

CASE C.J. a KING D.L., *Phsihng for undergraduate students*, Research in Higher Education Journal, 2008, strana 100-6.

Krátce z historie Internetu [online]. Brno: Masarykova univerzita, 2011 [cit. 2013-02-07] Dostupné z http://www.ics.muni.cz/bulletin/articles/22.html

Jak starý je internet [online]. 2013 [cit. 2013-02-07]
Dostupné z http://www.earchiv.cz/b13/b0101001.php3

Časová mapa českého Internetu [online]. 2002 [cit. 2013-02-07]
Dostupné z http://www.lupa.cz/clanky/casova-mapa-ceskeho-internetu/

Historie národní sítě pro vědu, výzkum a vzdělávání [online]. 2011 [cit. 2013-02-07]
Dostupné z http://www.cesnet.cz/sdruzeni/dokumenty/historie-narodni-site-pro-vedu-vyzkum-a-vzdelavani/

Internt a komunikace [online]. 2012 [cit. 2013-02-07]
Dostupné z http://www.czso.cz/csu/redakce.nsf/i/internet_a_komunikace