Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Katedra informačních technologií

Diplomant	:	**Pavel Koběrský**
Vedoucí diplomové práce	:	Ing. Libor Gála
Recenzent	:	

TÉMA DIPLOMOVÉ PRÁCE

Minimalizace nákladů spojených se spamem na straně příjemce

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a že jsem uvedl všechny použité prameny a literaturu, ze kterých jsem čerpal.

V Praze dne 5. 5. 2003 ....

podpis

Abstrakt

Cílem práce bylo vytvořit postup pro minimalizaci nákladů spojených se spamem na straně příjemce, který vychází z obecných údajů o spamu, analýzy nákladů, dostupných protiopatření a vlastního dotazníkového šetření.

Přínosem práce je shrnutí obecných informací o spammingu se zaměřením na ekonomické náklady a protiopatření, dále vlastní dotazníkové šetření zkoumající postoj veřejnosti ke spamu a k účinnosti protiopatření a aplikace těchto poznatků na metodologie informační bezpečnosti se zaměřením na fázi výběru protiopatření.

Úvodní část tvoří uvedení do problematiky spammingu, které obsahuje definice spamu, jeho klasifikaci, údaje o historii, současnosti a odhady budoucnosti spamu. Problém je zde dále analyzován z hlediska účastníků spamu a z hlediska technického provedení.

Druhá část nabízí pohled na spam z hlediska nákladů. Náklady související se spamem jsou rozděleny do třech kategorií – náklady přímé, náklady nepřímé a náklady na boj proti spamu – a analyzovány podle jednotlivých účastníků.

Třetí část obsahuje podrobnou analýzu dostupných možností obrany proti spamu. Opatření jsou rozdělena podle času působení na preventivní, dynamická a reaktivní. U každého druhu je uvedeno několik nejvýznamnějších metod obrany proti spamu.

Poslední část shrnuje předchozí části spolu s výsledky vlastního dotazníkového šetření a aplikuje je na metodologie informační bezpečnosti. Výsledkem je postup udržování informační bezpečnosti se zaměřením na výběr protiopatření, ke kterému jsou kromě podrobnějšího popisu uvedena také doporučení a kritéria výběru.

Abstract

This thesis was aimed at creation of process for minimization of spam-related costs on recipient's side. Process is based on basic information about spam, analysis of costs, analysis of available countermeasures and questionnaire survey.

There are three major contributions of this work. First one is process created by application of spam onto information security methodologies with accent on countermeasure selection phase. Second contribution is questionnaire survey targeted on public attitude to spam and effectiveness of countermeasures. Third one is summarization of known information about spam, especially about available countermeasures and costs related to spam.

Introductory part offers basic information about spam – definitions of spam, classification of spam, spam history, present state and future estimates. It also contains analysis of parties and technical aspects of spam.

Second part contains decomposition of spam-related costs on direct and indirect costs and countermeasure costs. These costs are further decomposed according to parties.

Third part offers detailed analysis of available spam countermeasures divided into three groups: preventive, dynamic and reactive. For each group most important countermeasures are mentioned.

Last part puts together previous chapters together with survey results and applies them on information security methodologies. The outcome is process of maintaining information security with accent on countermeasure selection – this part also contains recommendations and selection criteria.

Obsah

Úvod

Téma práce

Tématem této práce je minimalizace nákladů spojených se spamem na straně příjemce. Nevyžádaná elektronická pošta (spam) je jev, který zejména v poslední době nabývá na důležitosti. Velký objem spamu přináší poměrně značné ekonomické náklady, navíc je spam pro uživatele elektronické pošty nepříjemný i dalšími způsoby. Tyto faktory bere většina uživatelů internetu v potaz, a tak ke spamu zaujímají odmítavý postoj; zejména náklady způsobené spamem je pak také nutí k zavádění protiopatření. Podobně jako začátek devadesátých let znamenal rozmach šíření virů, a tak i antivirových opatření, znamená přelom století rozvoj problematiky spamu, a tak i opatření proti spamu.

Důvodem výběru tématu práce byl zejména tzv. faktor obtěžování. První „vlnu“ spamu jsem v důsledku vlastní naivity zažil hned v počátcích mé práce s internetem a ani do současnosti se mi nepodařilo se s problémem úplně vypořádat. Každodenních několik desítek spamů mne však přinutilo se problémem více zabývat, začít sledovat vývoj situace a přemýšlet nad možnostmi obrany.

Cíl práce

Prvním cílem práce je zmapovat oblast spamu. Vzhledem k tomu, že je spamming relativně novým problémem, neexistuje (zejména v češtině) dostatek materiálů, které by se touto tématikou zabývaly komplexně. Cílem tedy bylo poskytnout náhled na obecnou problematiku, dále nabídnout pohled perspektivou ekonomických nákladů, a nakonec zmapovat dostupné možnosti obrany.

Hlavním cílem však bylo na základě těchto informací a zejména vlastního dotazníkového šetření zaměřeného na postoje českých uživatelů ke spamu a používaným způsobům obrany navrhnout v souladu s metodikami informační bezpečnosti doporučení pro omezení dopadu spamu, konkrétně zaměřena na postup a kritéria výběru protiopatření.

Obsah práce

Práce je rozdělena do čtyř kapitol. První kapitola mapuje samotnou problematiku spamu. Je zde definován spam, je stručně popsána jeho historie, klasifikace, současný stav a budoucí vývoj. Dále se tato část zabývá rozborem procesu spammingu podle účastníků a popisem procesu z technického pohledu.

Druhá kapitola nahlíží na spam jako na problém, který přináší všem účastníkům ekonomické náklady. Přímé a nepřímé náklady jsou zde rozebrány z pohledu účastníků, zvlášť jsou analyzovány náklady na boj proti spamu.

V třetí kapitole jsou analyzována možná protiopatření, která jsou rozdělena do třech skupin podle času jejich působení na preventivní, dynamická a reaktivní. Popisována jsou opatření organizační i technická s cílem zmapovat co možná nejširší oblast na úkor podrobnosti.

Poslední kapitola shrnuje předpoklady z předchozích kapitol, doplňuje je výsledky průzkumů a vlastního dotazníkového šetření a na základě těchto východisek se snaží v souladu s metodikami informační bezpečnosti navrhnout postup zavádění protiopatření se zaměřením zejména na postup a doporučení výběru protiopatření.

Metoda zpracování práce

Při zpracování práce jsem se opíral zejména o zdroje volně dostupné na internetu, zejména vzhledem k tomu že relativní novost a dynamika problematiky způsobují, že není dostupných mnoho knižních titulů (zejména v češtině), které navíc poměrně rychle zastarávají. Kromě serverů specializovaných na problematiku spamu byly výborným zdrojem také internetové magazíny a denní tisk. Několik zajímavých poznatků také přinesly připomínky, které mohli respondenti dotazníkového šetření připojit ke svým odpovědím. Pro část zabývající se spamem v kontextu informační bezpečnosti byla výborným zdrojem diplomová práce [37] a prezentace [38].

Před započetím psaní práce byla nejprve provedena rešerše v té době dostupných materiálů a po ujasnění konceptu práce byla vytvořena první verze osnovy, která pak byla modifikována pouze minimálně. Ve stejnou dobu byl vytvořen dotazník pro šetření, které na internetu probíhalo asi po šest týdnů. Během této doby jsem pracoval zejména na popisné části práce, po zpracování dotazníku pak na části metodické.

Požadavky na čtenáře

Na čtenáře nejsou kladeny větší nároky na znalosti problematiky spamu, naopak jsou zejména první kapitoly určeny k uvedení do oblasti. Určitá orientace v prostředí internetu (znalost základních služeb, zejména elektronické pošty, a znalost používané terminologie) je však vyžadována.

Práce je určena pro všechny zájemce o problematiku spamu, zejména však pro ty, kteří se správou elektronické pošty nebo IT obecně více zabývají – tedy například postmasterům, IT managerům, správcům sítě a podobně. Těm může metodická část posloužit jako východisko pro volbu a implementaci vhodných protiopatření. Pro ostatní čtenáře bude zajímavější spíše první část, která jim umožní blíže se seznámit s problematikou spamu.

1. Co je to spam?

1.1. Úvod kapitoly

Cílem této kapitoly je uvést čtenáře do problematiky spamu – nevyžádané pošty obtěžující uživatele. Uvádí několik definic problému a vymezuje rámec pro další část práce. Kapitola se dále zabývá původem slova spam, klasifikací spamu z hlediska média a z hlediska obsahu. Snaží se také nabídnout odpověď na otázku proč je spam problémem, analyzovat marketingový význam spamu a shrnout současný stav (ve světě i v ČR) a vývoj do budoucnosti.

Další část kapitoly rozebírá problém spamu z pohledu účastníků a z technického pohledu (jakým způsobem je spam rozesílán, jaké techniky sbírání adres a maskování uživatele se používají).

1.2. Definice spamu

Na jediné definici se podobně jako u většiny pojmů z oblasti internetu nedokázala internetová veřejnost shodnout a pravděpodobně ani shodnout nedokáže. Nejčastěji jsou jako znaky spamu uváděny tyto:

- zpráva je nevyžádaná (unsolicited),
- zpráva je odesílaná ve velkém množství (bulk),
- zpráva obsahuje komerční sdělení (commercial),
- příjemce odesílatele nezná nebo s ním nebyl v osobním kontaktu,
- náklady odesílatele jsou nesrovnatelné s náklady příjemce.

Konkrétní definice se s problémem vypořádávají různým způsobem. Například nezisková organizace Mail Abuse Prevention System LLC [1] definuje spam takto:

„Elektronická zpráva je ‚spam' tehdy, KDYŽ:

1. identita příjemce a kontext je irelevantní, protože zpráva je stejně použitelná na mnoho dalších potencionálních příjemců; A
2. příjemce ověřitelně nedal úmyslné, zřejmé a odvolatelné svolení s odesláním zprávy; A
3. přenos a příjem zprávy se příjemci jeví jako nepřiměřená výhoda pro odesílatele."

Český server Antispam [2] přináší tři definice, které se na problém spamu dívají nejen přes jeho vnější znaky, ale zaměřují se také na podstatu problému. První z nich byl převzat ze serveru spam.abuse.net:

„Provozovat spamming znamená zaplavovat Internet mnoha exempláři jedné a téže zprávy, ve snaze vnutit ji lidem kteří by jinak takovouto zprávu přijmout vůbec nechtěli. Většina spamů jsou obchodně zaměřené nabídky, často jde o nabídky pochybných produktů, o nabídky postupů na rychlé zbohatnutí, či o nabídky pololegálních služeb. Odesílatele přijde rozeslání takovýchto zpráv velmi lacino – většinu nákladů totiž platí příjemci a poskytovatelé přenosových služeb, a ne odesílatel."

Druhou je citát Vinta Cerfa, člověka, který se podílel na vývoji protokolu TCP/IP a je tak považován za jednoho z „otců internetu:"

„Spamming je zneužitím elektronické pošty a síťových news na Internetu. Může vážným způsobem narušit provoz veřejných služeb, nemluvě již o efektu, jaký může spamming mít na

systém elektronické pošty kteréhokoli jednotlivce. … Provozovatelé spammingu ve skutečnosti odnímají významné zdroje uživatelům a provozovatelům služeb, aniž by k tomu měli jejich souhlas, a to bez jakékoli kompenzace.“

Na stejné stránce se nachází ještě jedna zajímavá „definice“: „Spamming používaný k marketingovým cílům je o tom, jak přenést rozhodující část nákladů marketingových nákladů na někoho jiného.“

Cílem této práce však není rozhodnout o tom, která z definic je správná, ale směřovat uživatele k minimalizaci nákladů spojených se spammingem. Z tohoto důvodu budeme dále za spam považovat takové zprávy, které jsou *nevyžádané* a způsobují uživateli *zbytečné ekonomické náklady*.

1.3. Původ slova spam

Také o původ slova spam existují spory. S jistotou můžeme říci, že nevyžádaná pošta je pojmenována podle produktu firmy Hormel Foods, konzervy z vepřového masa ne nepodobné našemu „lančmítu“. Jeho název vznikl v roce 1937 spojením slov Spiced Ham, kořeněná šunka, pomocí veřejné soutěže; jeho autor byl odměněn sto dolary [3].

Existuje mnoho teorií o přenosu tohoto slova z konzervy na internetový fenomén. Podle jedné z nich uvedené v encyklopedii Webopedia [4] termín vznikl na University of Southern Califonia. Jeho autoři vycházeli z toho, že spam má stejné charakteristiky jako tato masová hmota:

- nikdo ji nechce a nikdy se na ni neptá,
- nikdo ji nejí, je to první věc, která bývá odsunuta na okraj talíře,
- někdy může být skutečně chutná, stejně jako je 1 % nevyžádané pošty užitečné i pro ostatní.

Jiná teorie poukazuje na scénku ze seriálu Monty Python Flying Circus [5], zejména na její část, kdy servírka v restauraci prezentuje hostovi nabídku jídel:

> „Well, there's egg and bacon; egg sausage and bacon; egg and spam; egg bacon and spam; egg bacon sausage and spam; spam bacon sausage and spam; spam egg spam spam bacon and spam; spam sausage spam spam bacon spam tomato and spam; spam spam spam egg and spam; spam spam spam spam spam spam baked beans spam spam spam or Lobster Thermidor a Crevette with a mornay sauce served in a Provencale manner with shallots and aubergines garnished with truffle pate, brandy and with a fried egg on top and spam.“

což je skupinou Vikingů kvitováno písní s textem: „Spam spam spam spam. Lovely spam! Wonderful spam!“

Analogie s internetovým spamem (host si navíc žádá jídlo, které spam neobsahuje) je zde naprosto zřejmá. Podle další teorie bylo slovo spam použito v tomto významu jako metafora v reakcích na jeden z prvních případů Usenetového spamu. Teorií je mnoho a o pravém původu slova již asi nikdy nepůjde rozhodnout.

1.4. Klasifikace spamu

1.4.1. Klasifikace spamu podle média

Podle média se dají rozlišit dva základní druhy spamu (podle [6]) – *usenetový* spam a *e-mailový* spam. Na Usenetu (Usenet je celosvětový distribuovaný diskusní systém, často nazývaný jako „news“) se problém objevil jako první a zde byl také pojmenován. Za spam zde byl dříve považován zejména příspěvek, který byl zaslán do velkého množství skupin, a to tak, že byla do

každé skupiny zaslána jedna kopie zprávy (tzv. EMP, Excessive Multi-Postings), což při velikosti spamové zprávy, počtu jejích kopií, počtu Usenetových serverů a tehdejších cenách za megabajt diskového prostoru a za přenos příspěvků znamenalo poměrně značné náklady. Usenet news však umožňují tzv. crossposting, kdy je zpráva připojena k více skupinám, ale fakticky existuje pouze v jedné kopii. Zde není nárok na zdroje takový, ale pro uživatele je to stále stejně nepříjemné, a tak pojem spam nahradil u tohoto případu původní pojem velveeta.

Druhým druhem spamu podle média je spam e-mailový. Zde jsou nevyžádané zprávy zasílány přímo do e-mailových schránek uživatelů, často jsou také zneužívány e-mailové konference (mailinglisty) nebo skupinové adresy (jako například all@doména.tld). Zprávy jsou většinou zasílány hromadně na několik desítek adres. Termínem „sliced spam“ se naopak označuje e-mailový spam, který je rozesílán jednotlivým uživatelům – předstírá tak, že je cílený a tak spoléhá, že může být v očích uživatelů vnímán jako méně vážný problém.

V současné době zatěžuje uživatele vzhledem k poklesu významu Usenetu, kterému problém spammingu nepochybně napomohl, zejména e-mailový spam. Z tohoto důvodu se budu v dalším průběhu práce zabývat *pouze e-mailovým spamem*.

1.4.2. Klasifikace spamu podle obsahu

Mezi spam můžeme podle omezení v kapitole *1.2. Definice spamu* (nevyžádané zprávy způsobující zbytečné ekonomické náklady uživateli) zařadit tyto druhy zpráv (a samozřejmě také mnoho dalších, protože ne všechny zprávy, které definici vyhovují, můžeme do jedné z těchto kategorií zařadit):

- *Reklamní zprávy* – nevyžádané reklamní zprávy jsou naprosto nejčastějším představitelem spamu. Spammer zasílá texty, které mají v důsledku přinést finanční nebo jiný prospěch jemu, nebo jeho klientovi.

  As seen on NBC, CBS, CNN, and even Oprah!
  The health discovery that actually reverses aging while burning fat.
  Without dieting or exercise!
  Forget aging and dieting forever!
  Claim Yours Now!
  Would you like to lose weight while you sleep!
  No dieting!
  No hunger pains!
  No Cravings!
  No strenuous exercise!
  Change your life forever!
  100% GUARANTEED!
  Get your free bottle here:
  Visit Us

- *Hoaxy* – řetězové dopisy obsahující nepravdivou informaci, které příjemce určitým způsobem nutí (apelují na jeho sociální cítění, informují o neexistujících počítačových virech nebo jiných hrozbách, upozorňují na neexistující služby zdarma, vysoké výhry a podobně), aby zprávu poslal dále. Často obsahují také návod na vyřešení situace (zbavení se viru a podobně), který uživateli většinou spíše uškodí, než pomůže.

  Poprve to bylo zaznamenano v Parizi. Pred nekolika tydny si sedla jedna osoba v kine na neco pichajiciho na sedadle. Když vstala, aby zjistila, co to bylo, nasla jehlu zapichnutou do sedadla, na ktere byl pripevnen vzkaz: "Prave si byl nakazen HIV".
  Kontrolni stredisko chorob zaznamenalo v posledni dobe mnoho podobnych pripadu v mnohych dalsich mestech i v PRAZE !!!

> Vsechny testovane jehly byly HIV pozitivni nebo obsahovaly zhoubny typ zloutenky. Stredisko taktez udava,ze takoveto jehly byly nalezeny i na verejnych bankomatech a hlavne v dopravních prostedcích MHD, prevazne v metru. Je vice nez pravdepodobne, ze jehly nastrkavaji HIV nakazeni narkomani. Zadame kazdeho, aby byl v takovych pripadech obezretny. Meli byste si pozorne prohlednout kazde verejne sedadlo/zidli s nejvetsi opatrnosti. Starostlivy vizualni pohled by mel stacit. Zaroven vas zadame, abyste tuto zpravu podali co nejvyssimu poctu vasich blizkych, pratel i znamych,ktere tak upozornite na toto nebezpeci.
> Je to velmi dulezite! Jen si pomyslete: muzete zachranit život jen tim, ze odeslete tuto zpravu dale.
> Prosim,venujte par sekund vaseho casu na odeslani tohoto odkazu dale.
> MUDr. Eva Bendová

- *Řetězové dopisy* – mají stejný účel jako hoaxy: přinutit adresáta, aby je odeslal dále. Kromě toho, že mohou znepříjemňovat život, jsou neškodné. Nejčastěji na příjemce apelují, že když je odešle dále, tak bude mít štěstí a podobně. Na principu řetězových dopisů funguje také naprosto běžné přeposílání zpráv obsahující vtipy, veselé obrázky a podobně.

> Třeba to funguje - a je to i celkem pravdivé.
> Ten nejhezčí kolovací dopis na světě, nad kterým bychom se měli opravdu zamyslet! Na tomto příběhu je opravdu něco pravdivého. Pro informaci: přečíst si ho trvá jen dvě minutky. Obětuj ten čas!!!
> Můj nejlepší přítel otevřel šuplík od komody své manželky a vyjmul v hedvábném papíru zabalený balíček. Nebyl to jen tak obyčejný balíček, bylo v něm krásné dámské spodní prádlo. On ten balíček rozbalil a zadíval se na to hedvábí a ty jemné krajky.
> "To jsem jí koupil, když jsme byli spolu poprvé v New Yorku. To mohlo být asi tak před 8 nebo 9 roky. Nikdy si to neoblékla. Chtěla si to obléci při zvláštní příležitosti. A teď, myslím, že je ten pravý okamžik". Přiblížil se k posteli a položil to hedvábné prádélko k jiným věcem, které byly připraveny pro pohřební službu. Jeho žena totiž zemřela. Pak se ke mě obrátil a řekl: "Neukládej nikdy nic na zvláštní okamžik. Každý den, který žiješ je zvláštní okamžik."
> A já stále dodnes myslím na jeho slova .. ta změnila můj život. Dnes čtu více a uklízím méně. Sednu si na balkon, kochám se přírodou a ignoruji plevel, který se rozrůstá mezi mými květinami. Trávím více času s rodinou, s mým partnerem, s mými přáteli a méně v práci. Pochopil jsem, že život je sbírka zkušeností, kterých si máme vážit. Od teď si už nic neschovávám na později. Denně používám své křišťálové sklínky. Když se mi chce, tak si obléknu mou novou koženou bundu i když jdu jen přes ulici do samošky. I můj nejdražší parfém použiji, když se mi zachce. Slova jako např. "jednou" nebo "při příležitosti" už v mém slovníku neexistují. Když to stojí za to, tak chci dělat, slyšet i vědět vše hned. Nejsem si jistý, co by žena mého přítele udělala, kdyby věděla, že už zítra nebude. "Zítra", které každý z nás bere na lehkou váhu. Myslím, že by určitě ještě zavolala své rodinné příslušníky a své blízké přátele. Třeba by i zavolala pár lidí, s kterými by urovnala pár nedorozumění a nebo by se i pár lidem omluvila za věci, které byly nevyjasněné. Odpustila by možná vše, čím jí kdo ublížil. Ta myšlenka, že by třeba ještě šla do čínské restaurace /její zamilovaná kuchyně/ se mi líbí.
> To jsou ty nevyřízené maličkosti, které by mě rušily, kdybych věděl, že mé dny jsou spočítané. Na nervy by mi také šlo, že vím, že se už nemohu sejít s přáteli, které jsem chtěl jednoho "vhodného" dne navštívit. Na nervy by mi také šlo, že vím, že již nenapíši dopisy, které jsem chtěl jednoho "vhodného" dne napsat. Že jsem svým milým dost často neříkal, že je miluji. Teď nepropasu, neodložím a neuložím nic, co mi dělá radost a co přináší smích do mého života. Stále si říkám,

že každý den je zvláštní. Každý den, každá minuta, každá vteřina je zvláštní. Dostaneš-li tento dopis, znamená to, že existuje někdo, kdo ti přeje něco dobrého. Jsi-li ale tak zaneprázdněný, že nemáš pár minut času přečíst a poslat toto poselství dále, protože "za chvíli, zítra, za týden....." je také dost času, možná už to nikdy neuděláš.
Tato Tantra přichází ze severní Indie. Udělej si trochu času na přečtení a zamyšlení. Je to Tantra, která přináší štěstí. Obíhá již dlouho kolem světa. Nenech si to poselství jen pro sebe. Tantra by měla být poslána do 96 hodin dále. Dávej pozor, co se ti dalších pár dní přihodí. I když nejsi pověrčivý, uvidíš sám.
Pošli tuto zprávu nejméně na 1 osobu: Tvůj život se zlepší..
na 2-4 osoby: Tvůj život se zlepší viditelně...
na 5-9 lidi: Tvůj život se zlepší i tvé cíle...
na 10-14 lidi: Obdržíš nejméně pět překvapení, během pár týdnů...
na 15- více: Tvůj život se drasticky změní a vše o čem jsi kdysi snil nabere podobu..

- *Pyramidová schémata* (takzvané letadlo) – jsou řetězové dopisy, které obsahují návod na vytvoření stromové struktury („pošlete zprávu dalším pěti lidem“) a následné přeposílání peněz, pohlednic, pivních tácků a podobně na vyšší úrovně pyramidy („zašlete deset dolarů na první adresu v seznamu“) pod vidinou zbohatnutí tím, že se i odesílatel s dalším přeposíláním dostane na vyšší místa v seznamu.

Hi Discover is a simple, yet brilliant system that will work for you and anyone in the world to get cash. HOW DOES IT WORK? The one-time expense is $38.00. There are six levels. All you need to do is refer 10 people, who in turn refer 10, six levels deep and you will have earned over 5 Million Dollars in cash; enough money that you will be "set for life". This cheat-proof mathematical system guarantees your success. 100% assured Satisfaction and if for any reason you are not happy, it's refundable. This Web site will expose a Referral Program "Hidden Factor" that will give you the ability to be SUCCESSFUL in this BEST and Fastest Networking System. Be sure to use the calculator available. Click on: http://reports.emarketplacedirect.com/pages/314457.html Join us now and receive your web site within a minute. You won't find this much value anywhere and it's only $38.00. Just look at some of what you get... @ You get your own web site hosted FREE! @ You get all the products/services to get traffic to your site! @ You get real time status for all of your referral sales! @ You control what name appears on your web site! @ You can put your own hit counter on your main page! @ You get a lead generation page that works great! @ You get step-by-step instructions on how to get started! @ The company pays you on time, every time! @ This is real and it works!" Sign up B4 your friends tell you. Sincerely Kristy Our FREE Secret Reports Explode Your Online Business. Discover How To Reach Millions. Go To: http://reports.emarketplacedirect.com/ Free.jsp/pages/314457.html

- *Scamy* – e-maily, pomocí kterých se odesílatel pokouší podvést adresáta. Nejznámějším případem je tzv. Nigerijský scam, ve kterém je adresát požádán o zprostředkování převodu velkého množství peněz za určitou provizi, avšak nejdříve musí poslat peníze na zajištění převodu. K finálnímu převodu však nikdy nedojde, ačkoliv scammer tyto peníze k dispozici má – je většinou propojen s mafií, která peníze dále využívá zejména na nákup drog v Thajsku a jejich pašování do USA. (některé zdroje, například [7], dokonce uvádějí, že jsou do celého podvodu zapojeni i členové nigerijské vlády). Podle televizního pořadu MacIntyre – Reportáž točená inkognito: Miliardové podvody [8], který byl uveden v České televizi v souvislosti s vraždou nigerijského diplomata jedním z podvedených, na dopisy nabízející možnost převodu milionových částek odpovídá asi 10 % oslovených a asi jedno

procento scammerům skutečně zaplatí – průměrná oběť asi 200 000 USD, nejvíce bylo zaznamenáno 6 000 000 USD (dá se ale očekávat, že tato čísla budou v případě oslovení elektronickou poštou znatelně nižší). Podle magazínu The Inquirer [9] tito scammeři v roce 2003 očekávají přínos v hodnotě dvou miliard dolarů, což z tohoto podvodu dělá druhé největší „odvětví“ v Nigérii.

DEAR FRIEND,
I AM MRS. SESE-SEKO WIDOW OF LATE PRESIDENT MOBUTU SESE-SEKO OF ZAIRE? NOW KNOWN AS DEMOCRATIC REPUBLIC OF CONGO (DRC). I AM MOVED TO WRITE YOU THIS LETTER, THIS WAS IN CONFIDENCE CONSIDERING MY PRESENT CIRCUMSTANCE AND SITUATION.
I ESCAPED ALONG WITH MY HUSBAND AND TWO OF OUR SONS JAMES KONGOLO AND BASHER NZANGA OUT OF DEMOCRATIC REPUBLIC OF CONGO (DRC) TO ABIDJAN, COTE D'IVOIRE WHERE MY FAMILY AND I SETTLED, WHILE WE LATER MOVED TO SETTLED IN MORROCO WHERE MY HUSBAND LATER DIED OF CANCER DISEASE. HOWEVER DUE TO THIS SITUATION WE DECIDED TO CHANGED MOST OF MY HUSBAND'S BILLIONS OF DOLLARS DEPOSITED IN SWISS BANK AND OTHER COUNTRIES INTO OTHER FORMS OF MONEY CODED FOR SAFE PURPOSE BECAUSE THE NEW HEAD OF STATE OF (DR) MR LAURENT KABILA HAS MADE ARRANGEMENT WITH THE SWISS GOVERNMENT AND OTHER EUROPEAN COUNTRIES TO FREEZE ALL MY LATE HUSBAND'S TREASURES DEPOSITED IN SOME EUROPEAN COUNTRIES.
HENCE MY CHILDREN AND I DECIDED LAYING LOW IN AFRICA TO STUDY THE SITUATION TILL WHEN THINGS GETS BETTER, LIKE NOW THAT PRESIDENT KABILA IS DEAD AND THE SON TAKING OVER (JOSEPH KABILA). ONE OF MY LATE HUSBAND'S CHATEAUX IN SOUTHERN FRANCE WAS CONFISCATED BY THE FRENCH GOVERNMENT, AND AS SUCH I HAD TO CHANGE MY IDENTITY SO THAT MY INVESTMENT WILL NOT BE TRACED AND CONFISCATED.
I HAVE DEPOSITED THE SUM OF EIHGTEEN MLLION UNITED STATE DOLLARS(US$18,000,000,00.) WITH A SECURITY COMPANY , FOR SAFEKEEPING. THE FUNDS ARE SECURITY CODED TO PREVENT THEM FROM KNOWING THE CONTENT. WHAT I WANT YOU TO DO IS TO INDICATE YOUR INTEREST THAT YOU WILL ASSIST US BY RECEIVING THE MONEY ON OUR BEHALF.ACKNOWLEDGE THIS MESSAGE, SO THAT I CAN INTRODUCE YOU TO MY SON (KONGOLO) WHO HAS THE OUT MODALITIES FOR THE CLAIM OF THE SAID FUNDS.
I WANT YOU TO ASSIST IN INVESTING THIS MONEY, BUT I WILL NOT WANT MY IDENTITY REVEALED. I WILL ALSO WANT TO BUY PROPERTIES AND STOCK IN MULTI-NATIONAL COMPANIES AND TO ENGAGE IN OTHER SAFE AND NON-SPECULATIVE INVESTMENTS. MAY I AT THIS POINT EMPHASISE THE HIGH LEVEL OF CONFIDENTIALITY, WHICH THIS BUSINESS DEMANDS, AND HOPE YOU WILL NOT BETRAY THE TRUST AND CONFIDENCE, WHICH I REPOSE IN YOU. IN CONCLUSION, IF YOU WANT TO ASSIST US , MY SON SHALL PUT YOU IN THE PICTURE OF THE BUSINESS, TELL YOU WHERE THE FUNDS ARE CURRENTLY BEING MAINTAINED AND ALSO DISCUSS OTHER MODALITIES INCLUDING REMUNERATION FOR YOUR SERVICES.

FOR THIS REASON KINDLY FURNISH US YOUR CONTACT INFORMATION, THAT IS YOUR PERSONAL TELEPHONE AND FAX NUMBER FOR CONFIDENTIAL PURPOSE AND ACKNOWLEDGE RECEIPT OF THIS MAIL USING THE ABOVE EMAIL ADDRESS.
BEST REGARDS,
MRS M. SESE SEKO

1.5. Proč je spam problematický?

Jedna z největších organizací, které bojují proti spamu, Coalition Against Unsolicited Commercial Email (CAUCE, [10]), zmiňuje několik základních důvodů, proč je spam problémem.

1. *Přenos nákladů* – tímto problémem se budu podrobně zabývat v kapitole *2. Náklady související se spamem*. V jednoduchosti se dá říci, že náklady spammera jsou zanedbatelné ve srovnání s celkovými náklady ostatních zúčastněných stran (ISP, provozovatelů mailserverů, uživatelů, firem atd.).
2. *Lest* – spammeři si jsou vědomi toho, že kdyby neklamali, nemají žádnou šanci. Uživatelé by jejich zprávy nečetli, obrana právní cestou by byla snadnější a podobně. Proto je lest hlavní metodou jejich práce.
3. *Mrhání cizími zdroji* – zasílání spamu znamená pro postižené subjekty zbytečnou zátěž, která navíc omezuje možnost vykonávat jejich primární činnost. Například velké množství zpráv může zahltit některému z uživatelů jeho schránku a znemožnit mu tak přijímat důležitější zprávy od jiných uživatelů.
4. *Snížení významu elektronické pošty* – v případě nedostatečné obrany proti spamu může dojít k situaci, kdy se uživatelé rozhodnou přejít k jiným metodám komunikace z toho důvodu, že e-mailová schránka zahlcená spamem, ve kterém se špatně hledají důležité zprávy, bude málo efektivní.
5. *Faktor obtěžování* – už pouhý fakt, že z několika zpráv, které si uživatel stáhne, pro něj osobně není žádná, je velice nepříjemný. Stejně tak každé vyrušení od soustředěné práce novou zprávou, která pro uživatele nemá žádnou hodnotu.
6. *Etika* – principy spamu odporují etice. Dochází zde ke lstem, uváděním v omyl a v podstatě také ke krádežím (zdrojů, přesunutí nákladů).

1.6. Marketingový význam spamu

Na to, jaký je marketingový význam spamu, existují rozporuplné názory. Samotná reklama prostřednictvím e-mailu je pravděpodobně velice účinná, pokud oslovuje přesně vybraný segment uživatelů, kteří navíc souhlasí s tím, že budou reklamní zprávy od konkrétního subjektu dostávat, nebo s ním alespoň byli v předchozím kontaktu. Jiří Hlavenka v knize Internetový marketing [11] uvádí, že internetovému obchodu Vltava zvedá rozeslání cílených reklamních zpráv dřívějším zákazníkům nákupy až na 300 %. Z oslovených uživatelů reaguje 30 % do třech dnů, do týdne je to 80 %. I další zdroje uvádějí hodnoty, které potvrzují, že přestože se s množstvím zpráv účinnost e-mailové reklamy snižuje, stále je účinnější než proužková reklama na webových stránkách (ve srovnání podle CTR (click-through-ratio) – poměr reakcí k oslovením) a při vhodném cílení je jedním z nejúčinnějších druhů reklamy vůbec.

Spam takto jednoznačně pozitivní výsledky nemá. Studie ukazují velice nízkou, někdy i nulovou účinnost. Jako jeden z hlavních důvodů nízké účinnosti lze považovat fakt, že uživatelé dostávají poměrně velký objem reklamních (vyžádaných i nevyžádaných) zpráv, a tak jim věnují stále méně času. Dalším důvodem je pocit uživatelů, že jsou reklamou obtěžováni.

Vzhledem k tomu, že je spam rozesílán na tisíce e-mailových adres, nedá se očekávat, že by zde existovalo nějaké cílení reklamy na konkrétní segmenty uživatelů. Paradoxně účinnost spamu oslabuje také to, že si na něj lidé postupně začínají zvykat – dříve (i když v ČR i v současnosti – viz popis kauzy Tvujdum.cz v kapitole *3.4.1. Právo*) jedna e-mailová zpráva způsobila nespokojenost, uživatelé zprávy otevírali, aby zjistili, kdo jim zprávu posílá a náhodně mohli zjistit, že obsahuje něco zajímavého (Stuchlík [12] považuje spam za ideální nástroj pro skandální propagaci). Jako paralela se nabízí televizní reklama vkládaná doprostřed pořadů, kterou nyní sleduje jen zlomek původního počtu diváků. Také se již relativně rozšířilo povědomí, že „slušné firmy" spam neposílají, protože by to pro ně byla negativní reklama, proto uživatelé od spamu nic seriózního neočekávají. Nízká účinnost spamu ve srovnání s jinými formami nevyžádané reklamy (například letáky ve schránkách) se dá také zdůvodnit tím, že „vyhodit" e-mailovou zprávu je snazší. V neposlední řadě život spammerům komplikují prostředky aktivní obrany proti spamu (viz kapitola *3. Analýza dostupných možností obrany*).

Přestože je často přínos pro spammera minimální nebo spíše záporný (negativní reklama, pokuty, soudní jednání), vzhledem k minimálním nákladům na rozesílání zpráv (viz kapitola *2. Náklady související se spamem*) je možné je rozesílat v obrovských objemech a návratnost tak může i při nízkém podílu reakcí překračovat náklady. Proto lze očekávat, že se se spammingem budeme potkávat i nadále.

1.7. Dosavadní vývoj a odhady do budoucna

Problém spamu se vyskytuje podstatně déle, než by se dalo čekat. První spam byl podle [13] odeslán (ještě v ARPANETu) již v roce 1978 jedním ze zaměstnanců firmy Digital Equipment a zval oslovené (všechny uživatele ze západního pobřeží USA) na představení nového počítače DEC-20. Na Usenetu se první spam objevil až v roce 1988. V roce 1993 se začala elektronickou poštou poprvé rozesílat pyramidová schémata. Za opravdový začátek velkých problému se spamem se obecně považuje „případ Canter a Siegelová" z roku 1994 – spam inzerující nabídku zprostředkování povolení k pobytu v USA rozeslaný do všech diskusních skupin na Usenetu. Od této doby objem spamu neustále narůstá, také díky tomu, že se v roce 1995 poprvé objevily nabídky na prodej seznamu e-mailových adres a první software na rozesílání spamu (spamware).

Odhady současného objemu spamových zpráv a jeho vývoje do budoucna z různých zdrojů se poměrně značně liší. Dva odhady počtu zpráv za rok v miliardách uvádím v tabulce 1:

Tabulka 1 – Odhady objemu spamových zpráv

Odhadce	*Současný stav*	*Odhad*	*Uvedeno v*
Radicati Group	840 (rok 2002)	5318 (2006)	[14]
Jupiter Research	140 (2001)	845 (2006)	[15]

Rozdíly mezi jednotlivými odhady jsou velmi vysoké, většina odhadů se ale shoduje na tom, že podíl spamu k běžným e-mailovým zprávám se pohybuje někde mezi 15 % a 45 %. Podobný výsledek prokázalo i dotazníkové šetření vytvořené pro tuto práci (viz kapitola *4.3. Vlastní dotazníkové šetření*). Odhady se shodují také na tom, že tempo růstu objemu spamu překračuje sto procent ročně a přestože vysokým tempem roste také počet všech e-mailových zpráv, roste také podíl spamu k běžným zprávám. Pohled do budoucnosti je tedy v oblasti spamu (a tak i celé e-mailové komunikace) poměrně pesimistický.

1.8. Spam v České republice

Situace v České republice je nejen podle [16] od téhož jevu v USA (který se však projevuje celosvětově) diametrálně odlišná. Objem rozesílaného spamu je v poměru na počet uživatelů

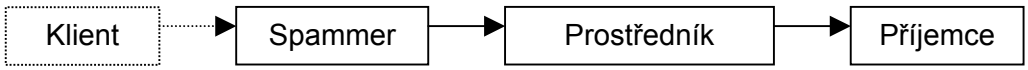
podstatně nižší. Spamové zprávy jsou rozesílány na malé množství adres, které většinou nejsou získávány strojovým sbíráním z webu nebo z komerčních seznamů adres, ale spíše jsou ruční prací spammera. Příjemce tak tvoří zejména známí známých spammera (který adresy získal z hlavičky hromadného e-mailu), odborníci v určité oblasti (spammer prochází například internetové magazíny zabývající se určitými tématy a sbírá jména redaktorů a čtenářů přispívajících do diskusí), nebo z jiných stránek, na kterých je uvedeno větší množství uživatelů s e-mailovými adresami (například seznamy spolužáků). Lze tak odhadnout, že spam v ČR je o něco lépe cílený a tak může dosahovat poměrně značné účinnosti (také protože jej uživatelé odlišují od spamu zahraničního). Rozesíláním spamu se ve většině případů nezabývají profesionální marketingové agentury, spíše je to otázkou malých firem. Často si uživatelé ani neuvědomují, že dělají něco špatného.

Výhodou České republiky v boji proti spamu je její poměrně malá velikost. Spammer tak riskuje poměrně značnou negativní reklamu, navíc je snadnější bojovat se spammerem kontaktem s jeho ISP nebo právní cestou. Také český právní řád se problematikou spamu zabývá.

Jak to bude s českým spamem do budoucna se dá zatím těžko odhadnout. Současná forma spamu v malém bude jistě pokračovat, jestli však kontrolu převezmou specializované firmy a budou spamovat ve velkém je nejisté. Nedávné finanční potrestání spammera v kauze Tvujdum.cz (viz kapitola *3.4.1. Právo*) však dává naději, že by spammeři mohli mít svou práci minimálně ztíženou.

1.9. Účastníci spamu

Účastníky spamu můžeme rozdělit do čtyř skupin podle rolí, které v celém procesu hrají. Vzhledem k tomu, že spam můžeme chápat jako jednosměrnou komunikaci, dá se proces vyjádřit jednoduchým lineárním grafem (viz obr. 1).



Obrázek 1- Účastníci procesu spammingu

Klientem chápeme zadavatele reklamy, většinou jde o firmy nebo podnikatele, ale zadavateli mohou být i jiné subjekty, například politici, umělci atd. Vzhledem k tomu, že klient může být zároveň spammerem, je v grafu znázorněn tečkovaně.

Spammer je subjekt, který zprávy rozesílá. Spammerem může být:

- *Jednotlivec* – spam může být rozesílán jednotlivci, jejichž hlavní činnost není většinou se spammingem spojena. Příkladem může být například pracovník malé firmy, který upozorňuje na její nový produkt, nebo třeba hacker upozorňující na svou stránku s ilegálním obsahem. Jednotlivci ale také samozřejmě mohou být ti, kteří se spamem zabývají jako hlavní (i když většinou ilegální) činností.
- *Spam gangs* – více než 90 % spamu rozesílaného uživatelům v Severní Americe a Evropě (podle [17]) ke rozesíláno skupinou zhruba dvou set „profesionálů“ (většinou s bohatou kriminální minulostí), seskupených do „gangů“.
- *Spamhau*s – tímto slovem se pejorativně označují ISP (Internet Service Provider, poskytovatel připojení k internetu), kteří tolerují rozesílání spamu ze svých serverů. Ve většině případů jsou těmito ISP přímo spammeři, kteří následně svádějí odeslané zprávy na své, většinou neexistující, zákazníky. Velkými ISP jsou takovíto poskytovatelé tolerováni, protože jim přinášejí peníze za pronájmy linek.

Mezi spammerem a příjemcem se vždy nachází několik *prostředníků*, kteří jsou do celého procesu většinou vtaženi nedobrovolně. Mezi tyto prostředníky mohou patřit například:

- *provozovatelé mailových serverů*, jež spammer zneužívá, nebo spamhaus;
- *správci linek, po kterých je spam přenášen* – ti nesou část nákladů na přenos dat;
- *ISP příjemce* – také nese náklady na přenos dat, často také za jejich uložení (může hostit e-mailovou schránku uživatele);
- *provozovatel poštovní schránky příjemce* – komerční služba nebo freemail (poskytovatel e-mailové schránky zdarma) musí spam uložit na svých serverech, freemaily jsou často zneužívány k rozesílání spamu;
- *e-mailové konference* – jsou zneužívány ke snadnému a spolehlivému rozšíření spamu mezi více uživatelů.

Za *příjemce* spamu můžeme z různých pohledů považovat různé subjekty:

- *jednotliví uživatelé* – ve svých klientech nakládají se spamem, stahují zbytečná data;
- *firmy* – provozují poštovní servery, platí zaměstnance, kteří jsou v důsledku spamu méně produktivní;
- *správci poštovních serverů* – zabývají se protiopatřeními.

1.10. Techniky, které spammeři používají

Rozesílání spamu je vždy nežádoucí a často také nelegální činnost, a tak jsou spammeři nuceni svou činnost určitými způsoby maskovat. V této kapitole stručně nastíním, jak vypadá technické provedení rozesílání spamu.

1.10.1. Způsoby rozesílání spamu

Existují čtyři hlavní způsoby rozesílání spamu podle druhu serverů, které spammer za tímto účelem používá:

- spamhausy,
- open relay servery,
- jednorázové účty u ISP,
- jednorázové účty na freemailech.

Jak bylo uvedeno výše (viz kapitola *1.9. Účastníci spamu*), *spamhausy* jsou ISP, kteří tolerují rozesílání spamu. Ve skutečnosti jsou většinou vlastníky spamhausu přímo spammeři. Článek Mika Wendlanda [18] o jednom z nejslavnějších spammerů Alanu Ralskym dobře ilustruje mechanismus rozesílání. Dvacet počítačů v sídle Alana Ralskyho kontroluje 190 poštovních serverů (které patří spamhausům), ze kterých se 30 nachází mimo USA (tyto servery patří místním ISP a je jim za službu řádně zaplaceno), každý server je schopen odeslat asi 650 tisíc zpráv za hodinu.

Velký podíl odeslaných spamových zpráv mají na svědomí *open relay servery* – servery, které umožňují třetí straně (tedy nejen lokálním uživatelům) odesílat e-maily jiným subjektům na internetu. Spammeři tedy tyto servery zneužívají (doslovný překlad anglického termínu relay rape by mohl být „znásilňují“) tím, že se k ním připojují a rozesílají velké množství zpráv. Správce serveru může tomuto jevu zabránit tím, že omezí možné odesílatele zprávy například podle IP adres nebo tím, že bude vyžadovat autentizaci.

Někteří ISP nabízejí možnost připojení k internetu zdarma – buďto trvale nebo na zkoušku. Spammer si takovýto *jednorázový účet* vytvoří (většinou pod falešnou identitou), připojí se

k němu a rozešle přes něj během několika hodin (většinou dokud nezareaguje ISP) několik tisíc zpráv. Pak celý proces opakuje s novým účtem.

Variací na jednorázové účty u ISP jsou *jednorázové účty na freemailech*. Na serveru poskytujícím e-mailovou schránku zdarma si spammer vytvoří účet a rozešle zprávy.

1.10.2. Způsoby maskování

Pokud by spammer odesílal zprávy stejným způsobem, jakým je odesílá běžný uživatel, bylo by to nejen neefektivní, ale také by o sobě prozradil příliš mnoho údajů, které by pak mohly vést k jeho dopadení.

Nejčastějším způsobem maskování spammerů je falšování hlavičky (header forging). E-mailová zpráva je uvozena hlavičkou, která obsahuje například údaje o odesílateli, příjemci, předmětu zprávy, jednotlivých serverech, které si zprávu předaly, nebo například kódování textu. Některé z těchto údajů lze s dobrou znalostí protokolu SMTP (Simple Mail Transfer Protocol) poměrně snadno zfalšovat, navíc software, který spammeři používají k rozesílání zpráv (tzv. spamware), má většinou tyto funkce již vestavěny.

Pravděpodobně každý příjemce spamu si všiml, že adresa, ze které spam přišel, vypadá podivně a e-maily na ni odeslané se vracejí. Spammeři totiž odesílají zprávu označenou (ve zfalšované položce hlavičky *From:*) například neexistující e-mailovou adresou, adresou třetí osoby (která je v celé věci naprosto nevinně a od postižených si většinou schytá svoje) nebo adresou jednorázového účtu, který však již byl provozovatelem zrušen. Odeslat zprávu pod zfalšovanou adresou není vůbec žádný problém a tak je většina spammerů z tohoto pohledu chráněna. Stejná adresa by se měla také vyskytovat v položkách *Return-path:*, *Sender:* nebo *Reply-to:* (ta bývá v některých případech skutečná, aby dal spammer oslovenému možnost odpovědět na jeho nabídku).

Příklad:

```
From: Membership Services <wkkapass@mad.scientist.com>
Return-Path: <wkkapass@mad.scientist.com>
Sender: Membership Services <wkkapass@mad.scientist.com>
```

Server mad.scientist.com ani doména scientist.com ovšem vůbec neexistují. Navíc již samotné slovní spojení „mad scientist“ (šílený vědec) vyzývá k ostražitosti.

Pro identifikaci spammera jsou však nejdůležitější ty části hlavičky, které obsahují informace o přenosu zprávy mezi jednotlivými servery – položky *Received:*. Každá položka obsahuje zprávu o předání zprávy mezi dvěma servery, čte se odspoda nahoru.

Příklad korektních položek Received: v hlavičce:

```
Received: from vse.vse.cz ([146.102.16.2] verified)
  by vse.cz (CommuniGate Pro SMTP 3.5.9)
  with ESMTP id 5830849 for xkobp03@veverka.vse.cz; Fri,
    20 Dec 2002 16:37:36 +0100
Received: by vse.vse.cz (Postfix)
       id C19E124A61; Fri, 20 Dec 2002 16:37:35 +0100 (MET)
Delivered-To: xkobp03@vse.cz
Received: by vse.vse.cz (Postfix, from userid 2525)
       id 8BAA924A58; Fri, 20 Dec 2002 16:37:35 +0100 (MET)
Received: from postcard.cz (unknown [193.85.233.122])
       by vse.vse.cz (Postfix) with ESMTP id CE8A724A61
       for <xkobp03@vse.cz>; Fri, 20 Dec 2002 16:37:33 +0100 (MET)
Received: from localhost (localhost [127.0.0.1])
       by postcard.cz (Postfix) with ESMTP id AD2905A177
```

```
    for <xkobp03@vse.cz>; Fri, 20 Dec 2002 16:37:33 +0100 (CET)
Received: by postcard.cz (Postfix, from userid 0)
    id 58A2F5A178; Fri, 20 Dec 2002 16:37:32 +0100 (CET)
```

Na příkladu můžeme vidět, jak položka Received: vypadá. Ve většině případů obsahuje zejména identifikaci serveru, který zprávu odesílá (následuje za „from“; je zde uvedena tak, jak se server představil), server, který ji přijímá (následuje za „by“), příjemce zprávy (za „for“) a údaje o datu a čase. Aby spammer zamaskoval, odkud zprávu posílá, většinou se pokouší oklamat mailserver tím, že mu udá falešnou nebo cizí adresu. V závorce za názvem odesílajícího serveru však může být uvedena skutečná IP adresa a název serveru, ze kterého byla zpráva předána (tyto údaje doplňuje poštovní server); porovnáním obou lze zjistit, zda byla položka zfalšována.

Příklad:

```
Received: from hotmail.com (pri-050-b31.codetel.net.do [196.3.77.50]) by
vse.vse.cz (Postfix) with SMTP id 3C1A924846; Sun, 26 Jan 2003 01:09:35 +0100
(MET)
```

Na tomto příkladu vidíme, že spammer uvedl jako odesílající server *hotmail.com*, ale ve skutečnosti byla zpráva odeslána ze serveru *pri-050-b31.codetel.net.do* v Dominikánské republice.

Pokud je známá adresa odesílatele, je poměrně snadné pomocí nástrojů jako je *nslookup*, *whois* a podobně zjistit alespoň minimum informací o spammerovi. V Received: mohou být podezřelé také další údaje, zejména datum nebo čas.

Často je falšována také položka *Message-ID*:, která by měla obsahovat unikátní identifikaci zprávy. Formát této položky je podle RFC 2822 <unikátní řetězec>@<jméno serveru>. Unikátní řetězec je dosazen aplikací, která zprávu odesílá; každý systém na odesílání e-mailů má vlastní formát, proto je možné identifikovat spam podle toho, že má toto pole odlišný formát, než ten, který by odpovídal například konkrétnímu uvedenému freemailu. Podobně se může lišit také jméno serveru.

Příklad:

```
Message-ID: <015e43e47c4a$8378b2c3$3cd37ca0@nbldsw>
```

V tomto případě položka ani neodpovídá standardu RFC 2822.

Hlavička může obsahovat také velké množství dalších položek, které jsou většinou také snadno falšovatelné a slouží spíše ke svedení uživatele na falešnou stopu.

Spammer se může maskovat kromě falšování hlavičky také v konkrétním obsahu dopisu, například odvoláváním se na autoritu, uváděním dočasných e-mailových adres, telefonních čísel na mobilní telefony s předplacenou kartou a podobně. Toto ale není specifikum spamu, proto se těmito metodami nebudu zabývat.

1.10.3. Metody získávání adres

Aby mohl spammer rozesílat zprávy, musí nejprve získat adresy. Může si samozřejmě koupit databázi s adresami od jiného spammera, v mnoha případech si však spammeři získávají adresy sami. Ti, kteří rozesílají spamy v malém objemu, často cílené na velice úzkou skupinu osob, adresy většinou sbírají ručně. Velcí spammeři však adresy získávají strojově ve velkém (tzv. harvesting).

Pravděpodobně nejvíce e-mailových adres získají spammeři pomocí programů, které procházejí webové stránky a hledají odkaz typu „mailto:jméno@doména.tld“. Lze očekávat, že novější programy již hledají i mimo odkazy, dokážou dešifrovat i adresy typu „jméno(at)doména.tld“ nebo např. jméno@nospam.doména.tld“, dokážou obcházet pasti (stránky, které obsahují velké

množství neexistujících adres, nebo jich dokonce generují nekonečně mnoho) a podobně. Adresy mohou být sbírány i cíleně, například procházením odkazů z určité kategorie v katalogu stránek, nebo odkazů vyhledaných ve vyhledávači po zadání určitých klíčových slov. Kromě samotné e-mailové adresy se mohou sbírat také další informace (například URL stránek, jejich titulek, možné jméno a podobně), které jsou pak využívány při rozesílání spamu tak, že zprávy na první pohled vypadají jako odesílané individuálně, nebo k cílení spamu.

Dalším velkým zdrojem adres je pro spammery Usenet. Diskusní příspěvky na Usenetu jsou velice podobné e-mailovým zprávám a v hlavičce obsahují informace, ze kterých se dá získat adresa odesílatele, a také obsahují datum a čas odeslání příspěvku, které umožňují rozpoznat, které adresy jsou „čerstvé." Programy na získávání adres pracují podobně jako ty na vyhledávání na webu, vyhledávají nejen v hlavičce zprávy, ale také v textu, jsou schopny odstraňovat maskování a podobně.

Jinou možností je získávání adres z mailinglistů (e-mailových konferencí). Některé servery obsahují příkaz na vypsání všech uživatelů, které mají pro spammera o to větší cenu, že nejsou nijak maskovány a pravděpodobně je také většina z nich funkční. Jinou možností je odeslání zprávy, která obsahuje žádost o potvrzení příjmu, do konference – spammer tak dostane potvrzenky od velké části členů mailinglistu. Možností je také přímé rozesílání spamu do jednotlivých konferencí (navíc některé servery na požádání vypíší všechny mailinglisty, které jsou na nich provozovány).

Běžný uživatel internetu se často setkává s formuláři, které po něm vyžadují zadání jeho e-mailové adresy. Nikdy se však nedozví, jestli spammer nezískal jeho e-mailovou adresu právě touto cestou. Nebezpečné mohou být také tradiční „papírové" formuláře, které většinou bývají převáděny do elektronické podoby (spammeři mohou získávat například adresy, uvedené u registrované domény).

V připomínkách respondentů k dotazníku (viz *4.3. Vlastní dotazníkové šetření*) se několikrát objevily obvinění z prodeje databáze adres třetím stranám. Obviněny byly v mnoha případech konkrétní služby, zejména freemaily (u kterých podobné počínání navíc dává smysl). Jinou možností mohou být také krádeže adres, získání adres po napadení serveru a podobně.

Existuje ještě mnoho dalších způsobů získávání adres, jako například:

- z informací, které odesílá webový prohlížeč nebo FTP klient,
- z IRC nebo jiných chatů,
- pomocí služby finger,
- slovníkovým útokem nebo hádáním (například skoro na každé doméně existuje adresa info@doména.tld) a následným zařazením funkčních adres do seznamu,
- hrubou silou (zkoušením náhodných řetězců),
- z veřejných adresářů a mnoho dalších (viz například [19]).

Důležitou roli v procesu získávání a udržování databáze adres hraje samotný spam. Spammeři rozesíláním spamu mohou zjišťovat, které adresy jsou funkční a naopak. Většina spamových zpráv také obsahuje odkaz na vyřazení z databáze, který sice může v některých případech fungovat, ale většinou pouze spammerovi potvrdí, že uživatel tuto adresu skutečně používá a její „cena" tak vzroste.

1.11. Závěr kapitoly

O konkrétní definici spammingu nelze rozhodnout, ale pro účely této práce budou za spam považovány takové zprávy, které jsou nevyžádané a uživatel způsobují zbytečné ekonomické náklady.

Spam je možné podle média klasifikovat na spam e-mailový a usenetový. E-mailový spam je vážnějším problémem a proto se tato práce bude zabývat právě jím. Podle obsahu je možné spam klasifikovat do poměrně značného množství druhů, mezi nejdůležitější patří reklamní zprávy, hoaxy, řetězové dopisy pyramidová schémata a scamy.

Za hlavní důvody, proč je spam problémem, se považuje přenos nákladů, časté využívání lsti spammery, mrhání cizími zdroji, snižování významu a využitelnosti elektronické pošty, faktor obtěžování a problémy související s etikou.

Na marketingový význam spamu existuje velké množství protichůdných názorů. Zatímco dobře provedený legitimní e-mailový marketing se považuje za poměrně účinnou metodu propagace, spam se díky vysokému objemu, faktoru obtěžování, minimálnímu cílení, ignorování spamu uživateli a rozšiřujícím se protiopatřením za účinný prostředek podle reakcí na oslovení považovat nedá. Vzhledem k minimálním nákladům a vysokému objemu však může být pro spammera ekonomicky zajímavý.

Ačkoliv se první případy spamu objevily už v sedmdesátých letech, rozmach přišel až v posledním desetiletí. Podle odhadů do budoucna lze očekávat stále vysoký růst objemu spamu, jehož tempo pravděpodobně překračuje i tempo růstu objemu e-mailové komunikace. Domácí spam v ČR není zdaleka takovým problémem jako spam zahraniční, většina spammerů rozesílá zprávy pouze v malém objemu a poměrně cíleně.

Účastníky spamu tvoří strana, která spam rozesílá (klient a spammer) a strana, která jej přenáší a přijímá (prostředník a příjemce). Spamy jsou většinou rozesílány pomocí vlastních nebo spolupracujících serverů spammera (spamhausy), přes cizí poštovní servery, které umožňují open relay nebo přes jednorázové účty u ISP nebo na freemailových službách. Identita spammera je ve většině případů maskována pomocí zfalšovaných položek v hlavičce. Adresy obětí spammer získává například z webových stránek, Usenetu, e-mailových konferencí, formulářů, nelegálními postupy (prodej, krádež, napadení serveru), útoky pomocí slovníků nebo hrubé síly a dalšími způsoby. Databázi adres spammeři udržují také pomocí zpráv serveru po odeslání zpráv a případných reakcí oslovených.

2. Náklady související se spamem

2.1. Úvod kapitoly

V této kapitole se pokusím o pohled na rozdělení nákladů souvisejících spamem, a to nejen na straně příjemce, ale také na straně odesílatele a prostředníků (viz kapitola *1.9. Účastníci spamu*). Náklady jsou analyzovány ve třech perspektivách – přímé a nepřímé náklady související se spamem a náklady na boj proti spamu (které jsou technicky součástí nepřímých nákladů).

2.2. Specifika nákladů souvisejících se spamem

Největším specifikem nákladů souvisejících se spamem je to, že zde existuje obrovský rozdíl mezi náklady spammera a náklady ostatních účastníků – náklady spammera na rozesílání zpráv jsou minimální, zatímco se spamem způsobenými náklady, které náklady na odeslání vysoce překračují, se potýká mnoho dalších účastníků. Celkové náklady jsou tak velké, ale zároveň jsou po rozpočtení na jednotlivé účastníky často příliš malé nato, aby se vyplatilo se spammery ve větší míře bojovat. Toto je hlavní důvod proč mají spammeři stále volné pole a jsou schopni své operace ještě více rozšiřovat.

2.3. Přímé náklady způsobené spamem

Za přímé náklady jsou v této kapitole považovány náklady na odeslání, přenos a příjem spamové zprávy (a další náklady, bez kterých by odeslání spamu nebylo možné), které jsou na jednoho příjemce z principu zhruba stejné, jako náklady u kterékoliv jiné e-mailové zprávy. Rozdíl je však v tom, že zatímco běžné e-mailové zprávy jsou většinou rozesílány na jednotlivé adresy, spamy jsou rozesílány řádově vyššímu počtu uživatelů, proto se zde dramaticky liší poměr nákladů na straně odesílatele k nákladům ostatních účastníků. Náklady zde budou analyzovány podle jednotlivých účastníků spamu (viz kapitola *1.9. Účastníci spamu*).

2.3.1. Klient

Náklady *klientů* tvoří náklady na vytvoření zprávy a platby spammerům za rozeslání zpráv. Spammeři si většinou účtují peníze podle počtu adres, na které zprávu rozešlou. Mezi cenami jednotlivých spammerů jsou poměrně značné rozdíly, zdůvodňované zejména kvalitou používaných seznamů (cílení, funkčnost adres a podobně), a proto nemá smysl zde uvádět konkrétní hodnoty, ceny také s velkým množstvím zpráv klesají na zlomek ceny při malém množství. Firma Jupiter Media Matrix (citováno v [20]) se v roce 2001 pokusila odhadnout náklady klientů na legitimní e-mailový marketing (tedy nikoliv spam) na jednu miliardu dolarů, a odhadla také jejich výši v roce 2006 na 9,4 miliardy dolarů. Jaká však může být výše nákladů firem na rozesílání spamu pravděpodobně není (také vzhledem k nelegalitě takovéhoto počínání) možné odhadnout. Pravděpodobně však bude ve srovnání s legitimním e-mailovým marketingem o poznání nižší.

2.3.2. Spammer

Mezi nákladové položky *spammerů* se počítají zejména tyto:

- *Připojení spammera k internetu* – tato položka není příliš vysoká, neboť kapacita samotné linky spammera nemusí být nijak velká – servery, ze kterých jsou velké objemy zpráv (a tak i velké objemy dat) odesílány, se ve většině případů nacházejí až na páteřní síti.

- *Provoz poštovního serveru* – spammeři mohou provozovat vlastní poštovní servery (tzv. spamhaus), u nich musí platit za hardware, software, údržbu a připojení k páteřní síti.
- *Platby externím ISP* – vzhledem k tomu, že v některých zemích není legální rozesílat spam, nebo vzhledem k možnostem úspor z rozsahu, si platí často spammeři provoz poštovních serverů u tolerantních (často specializovaných) ISP, kteří se v mnoha případech nacházejí v jiných zemích (offshore).
- *Náklady na získávání e-mailových adres* – aby mohl spammer zprávy rozesílat, musí mít k dispozici seznam cílových adres. Seznam si buď může koupit, nebo si jej může pořídit sám – to přináší další náklady na software sbírající adresy, provoz databáze adres, jejich verifikaci a podobně.
- *Pořízení a provoz hardware* – požadavky na hardware pro odesílání spamu jsou poměrně nízké, přesto to může být zejména u velkých spammerů poměrně signifikantní nákladová položka.
- *Pořízení software* – na trhu je poměrně mnoho produktů pro odesílání spamu (spamware), stejně jako u většiny ostatního software jsou některé komerční, jiné naopak dostupné zdarma. Velcí spammeři si většinou tento software vyvíjejí sami.
- *Další provozní náklady* – platy, pronájmy prostor, provoz webových stránek, telefony a podobně.

Pokud se nad těmito položkami zamyslíme podrobněji, je zřejmé, že po pořízení zařízení a software pro odesílání spamu tvoří náklady spammera pouze poplatky za připojení k internetu, případné poplatky za provoz poštovního serveru a běžné provozní náklady. Pokud se tyto náklady rozpočítají na velké množství zpráv, jsou náklady na jednu odeslanou zprávu velice nízké.

2.3.3. Prostředník

Většina nákladů způsobených spamem u *prostředníků* představují náklady na sníženou kapacitu. Přenos spamu zabírá kapacitu přenosových linek, která by jinak nebyla využita nebo byla využita jinak a tímto způsobem snižuje přenosovou rychlost. Spam (dočasně) uložený na serveru (v uzlových bodech, u ISP, provozovatele poštovních schránek) zase zabírá diskový prostor. Jakkoliv jsou tyto náklady na jednu zprávu velice nízké, při větším objemu zpráv (který například pro freemailový server může představovat několik set tisíc spamových zpráv denně) jsou náklady nemalé.

2.3.4. Příjemce

Na straně *příjemce* způsobuje spam zvýšení stávajících nákladů zejména v důsledku snížení kapacity (rozšíření kapacity připojení, rozšíření kapacity poštovních serverů, pevných disků a podobně) a přenosu zbytečných dat (zbytečné připojování, stahování spamů). Lze očekávat, že spam bude největší náklady přinášet právě příjemcům. Důvodů je několik:

- vzhledem k malému množství přenášených dat, použité technologii a podobně může být cena přenesení jednotky dat v poměru například k ISP vysoká (čas strávený připojením přes modem, data přenesená například přes GPRS, přeposílání zpráv na mobilní telefon přes placenou službu, stahování zpráv jen kvůli spamu);
- elektronická pošta může tvořit velkou část přenášených dat, proto bude velkou část tvořit i spam;
- spam může nutit ke zvýšení kapacity poměrně přesně dimenzovaných poštovních serverů.

2.4. Nepřímé náklady související se spamem

Za nepřímé náklady budeme považovat náklady, které souvisí se spamem, ale nejsou nutné pro jeho odeslání, přenos a přijetí.

Na straně *klienta* tvoří tyto náklady zejména náklady na zpracování reakcí oslovených uživatelů (stahování pošty, provoz bezplatných telefonních linek, zvýšení kapacity klientského centra), dále například náklady na výběr vhodného spammera a podobně.

Vzhledem k pokrokům v právní sféře tvoří často velmi vysoké položky v nákladech *spammera* náklady na soudní řízení a případné pokuty nebo jiné tresty. Jako u každého jiného podnikatele budou náklady tvořit další položky jako je například marketing, administrativa a podobně – prakticky všechny nákladové položky spammera kromě těch uvedených v přímých nákladech (kapitola *2.3. Přímé náklady způsobené spamem*) je možné považovat za jeho nepřímé náklady. Za „náklad“ spammera se dá počítat také pokles jeho příjmů, který je způsobený poklesem účinnosti reklamy v důsledku zavádění protiopatření na straně prostředníků a příjemců.

Asi největším nepřímým nákladem *prostředníků* je vyřizování stížností uživatelů. Ačkoliv ve většině případů za rozesílání spamu nemohou, jsou ze strany uživatelů bombardováni stížnostmi. ISP, z jejichž serverů byly zprávy odesílány, jsou obviňováni z toho, že mohli odeslání zabránit, ostatní subjekty (provozovatelé poštovních serverů, provozovatelé mailinglistů a podobně) z toho, že neposkytují ochranu před spamem a podobně. Výše těchto nákladů se ukázala být jedním z nejdůležitějších faktorů, který přesvědčil ISP k zákazu rozesílání spamu z jejich serverů, přestože příjmy od spammerů byly také poměrně vysoké. Mezi další nepřímé náklady můžeme počítat také poškození dobrého jména (zejména u ISP).

Největší část nepřímých nákladů na straně *příjemce* je způsobena ztrátou produktivity – identifikace spamových zpráv a jejich mazání zabere nějaký čas. Další čas může zabrat například prohlížení odkazů obsažených ve spamu. K tomu všemu je třeba připočíst také dobu, za jak dlouho se uživateli podaří znovu se soustředit a vrátit se k původní činnosti.

2.5. Náklady na boj proti spamu

Náklady způsobené spamem uvedené v předchozí kapitole je možné do určité míry eliminovat níže zmíněnými prostředky (viz kapitola *3. Analýza dostupných možností obrany*) obrany proti spamu. Pořízení těchto prostředků a jejich provoz ovšem přináší další náklady, které lze technicky považovat za nepřímé náklady související se spamem. Je nutné porovnat, zda se implementace protiopatření vyplatí, nebo zda je vhodnější ponechat současný stav a s implementací počkat až na situaci, kdy náklady způsobené spamem převýší náklady na boj proti spamu.

I zde budou pravděpodobně největší náklady dány časem, který uživatelé nebo zaměstnanci stráví například těmito činnostmi:

- zaváděním a konfigurací software,
- přidáváním odesílatelů/serverů/klíčových slov na blacklist,
- používáním více e-mailových adres,
- zaváděním preventivních opatření,
- bojem právní cestou (podání, účast na řízeních),
- kontaktování spammera, jeho ISP,
- vyhledávání legitimních zpráv označených jako spam (false positives),
- výběrová řízení, schvalovací procesy a podobně.

Nemalou nákladovou položku budou tvořit také náklady na pořízení software, který umožňuje eliminovat spam, a případné posílení hardware.

2.6. Odhady nákladů způsobených spamem

V médiích se v poslední době objevilo několik odhadů nákladů, které spam způsobuje. Například podle odhadu firmy Ferris Research (citováno v [21]) z ledna 2003 dosahují celkové náklady na spam ve světě výše asi 11,9 miliard dolarů, z toho dopadá 8,9 miliardy na společnosti v USA, 2,5 miliardy na evropské společnosti a 500 miliónů dolarů na ISP. Studie se také pokouší o rozklad nákladů firem v USA – náklady způsobené ztrátou produktivity tvoří čtyři miliardy dolarů, 3,7 miliardy je věnováno na boj proti spamu a přímé náklady (pořízení výkonnějších serverů a větší šířky pásma) a zbytek (tedy 1,2 miliardy) tvoří zejména náklady na zvýšené nároky na podporu uživatelů.

Podle studie Gartner Group (citováno v [22]) stojí spam ISP 7,4 – 7,7 miliónů dolarů na milión uživatelů. Evropská komise v odhadu z ledna 2002 ohodnocuje náklady na spam v Evropské unii na deset miliard euro ročně. (v [23]).

Tomáš Přibyl z brněnské firmy AEC odhadl (v [24]) výši ztrát na produktivitě práce a internetovém připojení v České republice na desítky miliónů korun ročně. Petr Koubský odhadl pro časopis Euro [25] náklady českých společností na (řádově odlišných) 1,9 miliardy korun na základě mzdových nákladů půl miliónu kvalifikovaných zaměstnanců pracujících s počítači a věnujících patnáct minut týdně na vypořádání se s nevyžádanými zprávami.

2.7. Závěr kapitoly

Existuje velký nesoulad mezi výší nákladů na straně spammera a na straně ostatních účastníků – náklady spammera jsou nesrovnatelně nižší. Naopak škody způsobené jedním spammerem jednomu příjemci jsou tak nízké, že se individuální boj se spammery nemůže vyplácet.

Přímé náklady jsou tvořeny náklady na odeslání, přenos a příjem spamové zprávy a jsou z pohledu jedné zprávy a jednoho příjemce svou výší srovnatelné s náklady na běžnou e-mailovou zprávu. Spam je ovšem rozesílán hromadně na velké množství adres.

Nepřímé náklady jsou všechny náklady, které se spamem souvisí, ale nejsou nutné pro jeho odeslání, přenos a přijetí. Za nepřímé náklady lze také považovat náklady na boj proti spamu, které umožňují snížit přímé i jiné nepřímé náklady. Velikost těchto nákladů by neměla překročit snížení ostatních nákladů v důsledku zavedení protiopatření.

Absolutní velikosti nákladů je těžké odhadnout, pravděpodobně dosahují řádově desítek miliard dolarů. Spam proto lze z nákladového hlediska považovat za poměrně závažný problém.

3. Analýza dostupných možností obrany

3.1. Úvod kapitoly

Cílem této kapitoly je poskytnout co možná nejobsáhlejší přehled metod, které se používají ke snížení dopadu spammingu nebo úplnému zabránění přijímání spamu. Metody jsou rozděleny podle klasifikace protiopatření využívané v informační bezpečnosti na preventivní (předcházející hrozbě), dynamická (prováděna v čase hrozby) a reaktivní (reagující na hrozbu a omezující budoucí dopady).

3.2. Preventivní opatření

Ideálním způsobem, jak se vyhnout spamu, je chovat se tak, aby se e-mailová adresa nikdy nedostala spammerovi do rukou. Pokud už se tak stalo, dají se následky vhodným chováním alespoň minimalizovat. V této kapitole budou uvedena některá základní pravidla prevence spamu.

Spammeři získávají e-mailové adresy většinou z veřejně dostupných zdrojů. Když svou e-mailovou adresu nezveřejníte, můžete komunikovat například se svými známými, naopak zveřejnění vaší adresy v určitém kontextu (například na osobní webové stránce nebo v odborné diskusi) může přinést mnoho zajímavých kontaktů, ať již profesionálních nebo osobních. A také usnadníte práci těm, kteří se vás pokouší najít nebo vaši adresu zapomněli. Často je uvedení e-mailové adresy podmínkou pro využití některé ze služeb. Toto dilema je třeba vyřešit v rozumném poměru (bohužel je skoro stoprocentní bezpečnost nezveřejnění adresy vyvážena i negativy) a dobře se rozhodnout, kdy adresu vůbec zveřejňovat nebo kdy použít některou z jiných možností.

Před zveřejněním adresy je tedy nutné odpovědět si na tyto otázky:

- *Potřebuji vůbec zveřejnit svou adresu?* – vyváží riziko přínosy?
- *Stačí ji zveřejnit pouze dočasně nebo trvale?* – jde jen například o jednorázové zaslání hesla, nebo o dlouhodobý kontakt?
- *Mohu důvěřovat subjektu, kterému adresu předávám?* – mohu očekávat, že adresa nebude zneužita?

Podle odpovědí je snadné se rozhodnout, zda adresu vůbec zveřejňovat, a pokud ano, tak jakým způsobem. Následující odstavce obsahují některé tipy pro relativně bezpečné zveřejnění adres.

Jedním z nejjednodušších způsobů je používat více e-mailových adres – určit si jednu nebo více adres jako soukromé (primární), tyto adresy nezveřejňovat a dávat je k dispozici jen důvěryhodným subjektům (příbuzným, známým, obchodním partnerům, úřadům a podobně). Pro jiné účely (formuláře, diskuse, zveřejnění na webových stránkách, petice a podobně) založit druhou (sekundární) adresu, kterou je případně možno zrušit a vyměnit za jinou. K dispozici je mnoho tzv. freemailových služeb, kde si může kdokoliv založit libovolné množství e-mailových schránek. Freemaily také často obsahují funkce, které mohou proti spamu alespoň částečně ochránit (většinou minimálně filtrování příchozích zpráv podle různých kritérií, v některých případech i komplexní antispamovou ochranu). Používání více adres s sebou bohužel nese zvýšení nákladů na jejich kontrolu. Je také nutné důsledně dodržovat rozdělení adres – více nedůsledně používaných adres znamená ještě více spamu než v případě používání jediné adresy.

Zajímavou variací jsou takzvané „jednorázové“ (disposable) adresy – uživatel si založí u některého z poskytovatelů (například SpamMotel.com, Spamex.com a dalších) e-mailovou schránku, jejíž adresu ale nikdy nezveřejňuje. Ke každé schránce si však může založit libovolný

počet dalších adres, které však slouží pouze jako jiná adresa pro původní schránku. Uživatel si tak ideálně založí novou schránku pro každé zveřejnění adresy a v případě, že mu přes některou z adres začne chodit spam, může adresu bez problémů zrušit (nebo se adresa zruší sama po přijetí určitého počtu zpráv) a přijde tak pouze o zlomek zpráv, o které by přišel, kdyby používal pouze jednu alternativní adresu a musel ji zrušit.

Některé servery doporučují používat pro riskantní účely falešnou adresu. Toto chování je však nebezpečné v tom, že tato adresa může patřit někomu jinému (nebo někomu bude patřit v budoucnu), kterého by nevyžádané zprávy obtěžovaly. Proto se tento postup nedá doporučit.

Často používaným způsobem, který znemožňuje získat e-mailovou adresu robotům procházejícím webové stránky, je maskování adres (munging, mung = úmyslně zničit). Nejtypičtějšími příklady mungingu jsou adresy uváděné jako:

- jméno at doména.tld
- jméno@nospam.doména.tld
- jméno (at) doména (dot) tld

Aby byl běžný uživatel schopen adresu rozkódovat (a asi se to stejně všem uživatelům nepodaří), používá se několik základních schémat, které se ovšem naučili rozpoznávat i v současnosti již poměrně dost inteligentní roboti. Určitou úspěšnost tato metoda sice má, ale otázkou zůstává, zda úspěšnost vyváží způsobené komplikace.

O něco úspěšnější jsou další metody maskování, které jsou používány zejména na webu, který je pro spammery pravděpodobně nejlepším zdrojem adres. Jednou z možností je zakódovat e-mailovou adresu do HTML entit obsahujících ASCII kód znaku (&#xxx;, kde xxx je kód znaku v ASCII tabulce). Tradiční příklad jmeno@domena.tld tak bude zakódován takto:

```
&#106;&#109;&#101;&#110;&#111;&#064;&#100;&#111;&#109;&#101;&#110
;&#097;&#046;&#116;&#108;&#100;
```

Většina prohlížečů by měla adresu zobrazit správně, dá se však očekávat, že někteří roboti dokážou prohlédnout i tento trik. Na internetu jsou také dostupné skripty, které používají k zamaskování e-mailové adresy některý z šifrovacích algoritmů.

Často se také nahrazuje celý text adresy nebo jenom zavináč obrázkem – v prohlížeči podporujícím obrázky lze adresu přečíst, ale roboti ji přečíst nemohou. Samozřejmě, že obrázek nemůže být součástí běžného odkazu (mailto:) nebo nemůže mít e-mailovou adresu v ALT tagu (popisu obrázku pro textové prohlížeče). Tento způsob maskování také komplikuje život uživatelům, kteří tak musí adresu ručně přepisovat do mailového klienta.

Jinou možností je naopak neuvedení e-mailové adresy, ale zachování odkazu – ten pak pomocí skriptu na straně klienta (typicky JavaScript) nebo na straně serveru změní aktuální URL na mailto:jméno@doména.tld. Tento způsob naopak handicapuje ty uživatele, kteří na odesílání pošty nepoužívají běžného klienta, ale například webové rozhraní poštovního serveru.

Asi ideálním způsobem jak ochránit e-mailovou adresu a přitom umožnit uživatelům internetu kontakt z webových stránek je umístit na ně formulář, který odesílá svůj obsah na zvolenou adresu. Ale i tato možnost může být cílem zneužití, naopak odesílatel nemusí být ochotný zadat svou adresu do formuláře, kterému nemusí věřit.

Webmasteři by si také měli dávat pozor na to, aby adresy nezveřejňovali jiným způsobem – například někde v kódu stránky nebo URL.

Pro ostatní kanály získávání adres lze asi pouze doporučit adresu vůbec neuvádět, případně uvádět adresu alternativní. Správci by se také měli zamyslet, zda neexistují kanály, které by mohly vést k možnosti získat adresy – například finger, adresářové služby, instant messaging atd.

I tu nejlépe střeženou adresu neuchráníte, když ji zveřejní někdo jiný. Nejčastějším způsobem je rozesílání e-mailů na více adres. Při zadání adres všech příjemců do pole To: (Komu:) vidí každý z příjemců všechny adresy. V některých případech to může být výhoda, ve většině případů však nikoliv. Takovéto hromadné zprávy se také často přeposílají dále, často s plným seznamem příjemců překopírovaným do textu, a tak může být jen otázkou času, než se k adresám dostane spammer. Navíc podle vyjádření Úřadu pro ochranu osobních údajů může být toto počínání také trestné (viz *3.4.1. Právo*). Je proto vhodnější zadávat adresáty hromadné zprávy do pole Bcc: (slepá kopie), kdy adresát nemůže zjistit adresy dalších příjemců. Pokud však dostaneme e-mail s uvedenými adresami, je vhodné odesílatele upozornit na nesprávnost jeho počínání a poradit mu, jak toto obejít.

Pokud byla adresa zveřejněna bez vědomí uživatele na internetu, nebo ji třeba z neznalosti zadal do některého z adresářů a podobně, je vhodné adresu smazat, nebo o její vymazání požádat správce místa, kde se adresa nachází (mohlo také dojít k porušení zákona o ochraně osobních údajů, viz *3.4.1. Právo*). Vhodné je jednou za čas nechat vhodným internetovým fulltextovým vyhledávačem vyhledat existující adresy a pokusit se o jejich odstranění.

Bohužel i adresa, která nikdy nebyla zveřejněna, může být cílem spammerů pomocí útoků na poštovní server – spammer se pokouší na server zasílat velké množství zpráv a z odpovědí serverů je schopen poznat, které adresy jsou funkční. Ve většině případů útok probíhá jedním ze dvou způsobů:

- *Slovníkový útok* – spammer zkouší vkládat před zavináč slova ze slovníku; zejména nejčastěji používaných e-mailových adres (info, sales, webmaster, w3), křestních jmen, nejčastějších příjmení případně doplněných iniciálou a podobně.
- *Útok hrubou silou (brute force)* – spammer zkouší všechny náhodné kombinace písmen.

Proto je při rozhodování o podobě e-mailové adresy (případně politiky tvorby e-mailových adres) vhodné brát v úvahu i tyto možnosti útoku a volit raději adresy delší a méně snadno odhadnutelné. Poměrně účinnou obranou zde může být nastavení serveru, například omezení počtu zpráv odeslaných z jedné domény za určitý čas.

3.3. Dynamická opatření

Jak bylo uvedeno v kapitole *3.2. Preventivní opatření*, ani sebedokonalejší prevencí se nedá zabránit tomu, aby se e-mailová schránka stala terčem spammerů. Pokud taková situace nastane, je třeba zvolit některou z metod omezení současného dopadu těchto zpráv. V případě menšího množství zpráv je samozřejmě možné se k celé věci stavět pasivně, ale když uživatel dostává denně několik desítek nebo dokonce stovek nevyžádaných zpráv, je nutné zvolit razantní aktivní řešení. Tato kapitola by měla představovat přehled dostupných metod, které umožňují alespoň částečně snížit škody způsobené spamem.

3.3.1. Filtrování zpráv

V případě, že objem spamu vzroste tak, že by to pro uživatele znamenalo značnou ztrátu produktivity, je vhodné zavést některý ze způsobů filtrování zpráv – podrobení zpráv určitým testům, jejichž výsledkem by mělo být rozhodnutí o tom, zda je zpráva v pořádku, nebo je spam. V důsledku tohoto rozhodnutí se pak provádí některá z akcí:

- *Smazání zprávy* – zpráva je smazána, uživatel jí tak nemusí stahovat, ale přichází o možnost kontroly rozhodnutí.
- *Přesunutí zprávy do zvláštní složky* – po testu je zpráva přesunuta, uživatel ji tak musí stáhnout, ale má zpětně možnost zjistit správnost rozhodnutí, případně o zprávě získat další informace.

- *Označení zprávy* – zpráva je označena (například změnou předmětu zprávy nebo přidáním položky do hlavičky), uživatel pak může pomocí filtrů nebo pravidel o jejím osudu rozhodnout sám.

Vzhledem k tomu, že všechny spamové zprávy nejsou rozhodně stejné a nové vznikají každým dnem, žádný z automatizovaných testů nedokáže o tom, zda je zpráva spamem nebo ne, rozhodnout tak bezchybně, jako dokáže lidský mozek (i když i ten s tím může mít někdy problémy). Vzniká tak hrozba tzv. „false positives" – zpráv, které jsou testem považovány za spam, i když jsou naprosto legitimní (opakem jsou „false negatives" – spamové zprávy, které jsou považovány za legitimní). Tento problém tak může být největší brzdou zavádění opatření proti spamu, neboť legitimní zpráva, která se v důsledku falešně pozitivního testu nedostane ke svému příjemci, může nakonec způsobit náklady, které převyšují úspory vzniklé filtrováním spamu. Nastavení pravidel je proto většinou méně citlivé, než by bylo optimální, což snižuje přínosy filtrování. Výrobci produktů se snaží metody testování neustále zlepšovat, avšak i spammeři upravují své zprávy podle těchto pravidel (a navíc jsou jako „útočící" strana o krok napřed).

3.3.2. Fyzické modely

Existuje několik možností technického provedení filtrování zpráv. Vzhledem k tomu, že na straně příjemce tvoří dvě hlavní součásti systému pro příjem e-mailových zpráv e-mailový server a e-mailový klient, filtrování tak může probíhat na obou stranách; filtrování však také (vzhledem k povaze protokolů pro přenos zpráv) může provádět i externí subjekt.

Filtrování lze provádět na poštovním *serveru* nebo na vnější poštovní bráně – při doručení zprávy nebo periodicky je spuštěna specializovaná aplikace, který na nových zprávách provede sérii testů a pozitivní zprávy podrobí předem definované akci. Protože musí být testování podrobeny všechny příchozí zprávy (což může zejména v případě velkých serverů, například freemailů nebo centrálních serverů nadnárodních společností znamenat objem řádově v miliónech zpráv), klade tento model poměrně značné nároky na výkonnost serverů. Druhou nevýhodou tohoto modelu je nemožnost (nebo jen velice omezená možnost) zásahu do procesu testování individuálním uživatelem (customizace procesu). Druhou stranou mince jsou však značné úspory způsobené centrální administrací. Výhodou je také transparentnost pro uživatele a to, že opatření proti spamu tak využívají i uživatelé, pro které by individuální obrana znamenala příliš těžký úkol, a tak by se nebránili vůbec.

Protikladem tohoto přístupu je filtrování na straně *klienta*. Největší výhodou a zároveň i nevýhodou tohoto provedení je individuální správa pravidel, která sice přináší možnost ušít pravidla přesně na míru daného uživatele, náklady na administraci jsou však relativně vysoké, navíc efektivnost kontroly je ovlivněna zdatností uživatele (pokud si tedy málo počítačově gramotný uživatel vůbec takovýto systém nainstaluje). Existuje několik možností provedení filtrování na straně klienta:

- Aplikace provádějící filtrování je obsažena přímo v klientovi (jako jeho integrální součást, jako plugin a podobně) – série testů je provedena většinou po stažení zpráv. Tento způsob umožňuje plnou integraci s dalšími funkcemi klienta, navíc se dají očekávat nižší požadavky na výkonnost pracovní stanice.
- Aplikace provádějící filtrování je samostatný program a testům podrobuje zprávy uložené na serveru – aplikace si ze serveru stáhne buď jen hlavičky zpráv nebo celé zprávy, analyzuje je a na serveru provede úpravy podezřelých zpráv. Výhodou je nezávislost na klientovi (a většinou i na serveru). Nevýhodu přináší velká režie přenosu dat (přenáší se až dvojnásobek dat), náročnost na výkonnost pracovní stanice a zejména problémy se synchronizací – pokud klient stahuje novou poštu periodicky, může dojít k tomu, že stáhne poštu ještě nezkontrolovanou.

- Aplikace provádějící filtrování je samostatný program, stojí jako mezičlánek (proxy) mezi serverem a klientem, testy provádí při příjmu zpráv – klient při žádosti o stažení zpráv kontaktuje proxy, ta stahuje zprávy, kontroluje je a teprve následně je předává klientovi. Nevýhodou jsou větší požadavky na výkonnost, hlavní výhodou je transparentnost pro klienta a nezávislost na použitém klientovi/serveru.

Třetí možností je využívání služeb *externího subjektu*. Princip je podobný jako u možnosti klient-samostatný program-testování zpráv na serveru. Aplikace běžící na internetovém serveru třetí strany se periodicky připojuje k poštovním serverům uživatele, analyzuje na nich uložené zprávy a provádí jejich úpravy. Jako hlavní výhody tohoto přístupu můžeme charakterizovat nezávislost, transparentnost, nulové náklady na administraci a nulové zatížení vlastního hardware. Služby jsou však v drtivé většině případů placené.

3.3.3. Blacklisty

Spolu s vyhledáváním určitých klíčových slov je asi nejpoužívanější metodou vytváření tzv. blacklistů – seznamů uživatelů, od kterých nelze přijímat poštu (nebo je tato pošta označována jako podezřelá). Zprávy však nejsou filtrovány pouze podle e-mailových adres (jak bylo zmíněno v kapitole *1.10.2. Způsoby maskování*, bylo by to pravděpodobně poměrně neúčinné), ale také podle dalších informací o původu zprávy obsažených v hlavičce.

Nejjednodušší metodou filtrování adres podle odesílatele je porovnávání zakázaných e-mailových adres s adresou odesílatele uvedenou ve zprávě, nebo také porovnávání domén. Tento druh blacklistu se dá implementovat v podstatě na každém e-mailovém klientovi i serveru (většinou tyto produkty obsahují možnosti filtrování). Vzhledem k jednoduchosti metody jej využívají nejčastěji individuální uživatelé. Může být poměrně účinný proti malým spammerům, kteří adresy nemění příliš často nebo je nemaskují, nebo v případě, kdy uživatel dostává zprávy například od jediného spammera (z jedné domény). Pokud však uživatel dostává zprávy od velkých spammerů, je tato metoda v podstatě neúčinná, neboť adresy odesílatelů jsou ve většině případů zfalšované a neexistující a prakticky se neopakují. O něco větší účinnost skýtá filtrování podle domén – pokud spammer odesílá zprávy pouze z několika málo serverů, je možné tyto servery vyfiltrovat. Spammeři se proti tomuto brání tím, že spam odesílají z adres velkých freemailových serverů (Hotmail, Yahoo!Mail a podobně) a počítají s tím, že celou doménu uživatel nezablokuje, protože většina uživatelů má alespoň jednoho známého, který používá služeb jednoho z inkriminovaných serverů. Další možností je odfiltrování zpráv, které byly odeslány ze zemí (tedy mají top-level doménu některé země), ze kterých uživatel poštu běžně nepřijímá. Tato strategie může být účinná zejména v souvislosti s přesunem spammerů do zemí s méně striktními antispamovými zákony. Přesto je její účinnost značně omezená.

Protože (jak bylo zmíněno výše) náklady na správu individuálních blacklistů jsou poměrně vysoké, vznikají veřejné blacklisty, které dokážou obsloužit velké množství uživatelů, a tak jsou náklady ve srovnání s individuální správou nesrovnatelně nižší, navíc rozsah těchto blacklistů mnohonásobně převyšuje rozsah individuálních seznamů. Aby však blacklisty tohoto rozsahu dosáhly, jsou závislé na „udáních“ od uživatelů. I přes ověřování zde může vznikat problém nevinných obětí, serverů nebo odesílatelů, kteří jsou na seznam zařazeni bezdůvodně. Podobný problém představuje vyřazování „polepšených“ subjektů, zejména z důvodu časové prodlevy mezi synchronizací blacklistů (technicky je porovnávání realizováno buď jednorázovými dotazy na blacklist nebo stažením celé databáze a prováděním dotazů na lokální kopii). Pokud je blacklisting prováděn na základě IP adres, existuje zde také možnost, že poté, co spammer opustí zablokovanou IP adresu, je tato adresa přidělena někomu jinému, který je tedy opět nevinně zablokován. Systém vyřazování nevinných nebo polepšených subjektů je tedy minimálně stejně důležitý, jako systém zařazování nových „hříšníků.“

Jedním z největších blacklistů je Mail Abuse Prevention System (MAPS, mail-abuse.org), který nabízí placené přístupy do svých databází. MAPS provozuje zejména čtyři blacklisty (podle IP adres), které se liší podle typů blacklistovaných subjektů:

- *DUL* (Dial-up Users List) – seznam IP adres, které představují uživatele, kteří se připojují telefonicky. Tyto IP adresy nemusí být spammeři, jde zde spíše o to, že velká část spamu je odesílána přes tento typ připojení.
- *RSS* (Relay Spam Stopper) – seznam IP adres poštovních serverů, které umožňují open relay (viz *1.10.1. Způsoby rozesílání spamu*) a byl přes ně rozesílán spam.
- *RBL* (Realtime Blackhole List) – seznam IP adres, ze kterých byl odesílán spam nebo které spam tolerují nebo podporují (multi-hop open relay, spamhausy, webové servery, na které spammeři odkazují a podobně).
- *NML* (Non-confirming Mailing List) – seznam IP adres, na kterých jsou provozovány mailinglisty (e-mailové konference), které nesplňují podmínky verifikace uživatelů.

Většina dalších blacklistů je také založena na filtrování IP adres, blacklisty jsou nejčastěji zaměřeny na open relay servery (například *ORDB.org*) nebo původce spammerů (*The Spamhaus Project*).

3.3.4. Whitelisty

Opakem blacklistů jsou whitelisty – seznamy odesílatelů, pouze od kterých uživatel zprávy přijímá. Proti spamu je tento systém účinný stoprocentně, bohužel však za cenu toho, že uživatel nepřijme velkou část legitimních zpráv. Je proto nutné vyřešit způsob přidávání nových příjemců do whitelistu. Nejjednodušší možností je samozřejmě způsob, kdy uživatel přidává do whitelistu příjemce vlastnoručně. Tento způsob může fungovat pro případy, kdy je schránka používána pouze pro komunikaci s malým množstvím neměnných příjemců (ale i tehdy může tento způsob vytvářet problémy, například když některý z odesílatelů používá více adres a nemá vždy přístup ke všem). Je tedy nutné systém doplnit některým ze způsobů přidávání nových příjemců do seznamu. Tento způsob může být doplněn možností zasílání žádostí o autorizaci například na jinou e-mailovou adresu (nebo úplně jiným způsobem). Pohodlnější však může být, když je uživatel informován alespoň o adresátech příchozí pošty a může tak poměrně efektivně přidávat nové povolené odesílatele. Tento způsob však stále vyžaduje zásah uživatele, což kromě nároků na jeho čas způsobuje časovou prodlevu mezi dobou plánovaného zaslání zprávy a dobou skutečného doručení. Proto je nejvhodnější celou věc řešit automaticky, navíc pokud se uživatel chce bránit pouze proti spammerům (a ne proti skoro všem uživatelům elektronické pošty), znamená automatické ověřování značné zvýšení efektivity na obou stranách. Ověřování obecně probíhá takto:

1. Uživatel odešle e-mailovou zprávu.
2. Server mail přijme, uloží, a odešle zpět zprávu s pokyny pro ověření.
3. Uživatel splní pokyny.
4. Zpráva je doručena.

Rozdíly mezi jednotlivými metodami tvoří způsob samotného ověření (tedy bod 3). Nejjednodušší možností je pouhá odpověď na zprávu (často na jednorázovou adresu). Pokud je však spammer z tímto způsobem obeznámen (je například implementován na nějakém velkém freemailu), není pro něj problém odpovědi odesílat automaticky. Podobná situace je s klepnutím na odkaz, který předává přes webový server příkaz k přidání uživatele do whitelistu.

Proto většina používaných metod vyžaduje od potencionálního odesílatele určitou akci. Například opsání určitého textu z těla zprávy do jejího předmětu, opsání textu z obrázku

a podobně. Extrémní možností je využití tzv. Turingova testu. Turingův test (původně teoretická konstrukce z oblasti umělé inteligence) je úloha, kterou dokáže člověk snadno vyřešit, ale počítač ji vyřešit nedokáže (například rozpoznání rozmazaného textu na různobarevném pozadí). Turingův test tak umožňuje naprostou obranu proti strojovému spamování[1]. Stejně jako většina jiných možností vytváření whitelistu (snad kromě přidávání samotným uživatelem) však není účinná v případě malých spammerů. Výhoda whitelistu je ale v tom, že pokud se něčí chování adresátovi nelíbí, může jeho adresu permanentně ze seznamu vyřadit. Účinnost této metody je tedy velmi vysoká, ovšem za cenu transakčních nákladů spojených s ověřováním a rizika, že některé důležité zprávy nebudou doručeny nebo budou doručeny se zpožděním po manuální kontrole (analogie s „false positives“).

3.3.5. Analýza obsahu zpráv

Spamové zprávy obsahují mnoho společných prvků a tak jsou pro člověka většinou na první pohled rozpoznatelné. Metody analýzy obsahů zpráv této vlastnosti využívají ke strojovému rozpoznávání spamových zpráv.

Nejjednodušší metodou analýzy je vyhledávání klíčových slov nebo slovních spojení. Tato metoda je snadno realizovatelná na většině e-mailových serverů i klientů, a proto je velice využívaná zejména individuálními uživateli. Pokud je ve zprávě obsaženo některé z klíčových slov nebo slovních spojení, která uživatel neočekává a jsou často používaná ve spamech (například sex, xxx, viagra, free offer, make money fast atd.), je mail označen jako spam a je provedena určitá akce (označení, smazání, přesunutí do jiné složky a podobně).

Jiná klíčová slova mohou naopak sloužit jako polehčující okolnosti – například pro někoho úspěšné nastavení spamového filtru by třeba lékařům mohlo odfiltrovat velké množství legitimní pošty, a tak se současný výskyt jiného klíčového slova považuje za znak, že zpráva není spam.

Ideální je samozřejmě porovnávat celou zprávu s databází vzorů již dříve identifikovaných spamových zpráv. Protože však zejména formát zprávy nemusí být vždy stejný, je vhodnější porovnávat zprávu pouze proti delším segmentům textu.

Zda je zpráva spam může napovědět také analýza formátování zprávy. Velká část spamu je odesílána v HTML formátu, který obsahuje nejen samotný text zprávy, ale i informace o formátování. Strojově je možné identifikovat některé typické znaky spamů, jako jsou například velký poměr kódu k textu, používání velkého písma, barev, obrázků, malý poměr textu k obrázkům, velké množství odkazů a podobně. I obyčejné textové zprávy mohou být takto testovány, například na velký počet řádek napsaných velkými písmeny.

V extrémních případech může jednorázové filtrování (výskyt jednoho slova nebo fráze znamená pozitivní test) přinášet relativně dobré výsledky, běžně však tato metoda přináší poměrně značnou hrozbu false positives. Proto jsou využívány zejména systémy vah/vícekriteriálního hodnocení, které eliminují false positives při současném zvýšení úspěšnosti.

Bohužel na filtrování zpráv v poslední době poměrně účinně reagují i spammeři. Často se lze setkat se zprávou, jejímž obsahem je pouze obrázek. Člověk sice text na obrázku přečte, filtrovací algoritmus však nikoliv. A používat jako filtrovacího kritéria to, že zpráva obsahuje pouze obrázek nebo malý poměr textu ke grafice, je značně nepřesné.

---

[1] Turingův test by také mohl být využíván na straně klienta ke zvýšení kredibility zprávy označením při odeslání.

Spammeři se proti filtrům brání také úmyslnými překlepy slov, která bývají často filtrována. Následující příklad obsahuje patičku zprávy, jejíž obsah tvořil pouze obrázek se sdělením (překlepy jsou podtrženy).

Příklad:

> 99454524 Don't want to receive our emails anymore? It's very easy to oppt out. And yes, doing so really will allow you to opppt out. We aren't just saying that so that we can put on the facade that we're legitimate advertsers, whilst laughing away, blatantly ignoring remvve requests. If you remove your name from our list, you definitely will be remm,oved. Your name will be marked as r,emoved in our email database, and you won't receive mail again. We don't really know how more clearly we can explain this. Just take our word for it. Otherwise, continue toreceive these emails. Now is your chance to opp,t out. Do so by clicking this "UNSUBCRIBE" link. P.S. - It really works

3.3.6. Analýza hlaviček

Jak již bylo zmíněno v kapitole *1.10.2. Způsoby maskování*, spammeři používají některé techniky, které jim pomáhají zůstat alespoň v částečné anonymitě. Většina z nich se nějakým způsobem dotýká hlaviček zpráv a proto může být vyhledávání charakteristických znaků právě v hlavičkách poměrně účinným prvkem.

Jednou z možností je analýza adresy odesílatele – spammera může prozradit například to, že adresa neobsahuje skutečné jméno a naopak obsahuje velké množství číslic, zejména v kombinaci s doménou některého z velkých provozovatelů. Podobně také pole pro adresáty zprávy (To:) může leccos prozradit. Typicky tvoří obsah této položky několik desítek adres, v podstatě u žádné z nich není uvedené pravé jméno, naopak je jako pravé jméno uvedena část e-mailové adresy před zavináčem, adresy jsou si podobné (například jsou odesílány uživatelům na stejné doméně, kteří začínají od stejného písmene) a setříděné podle abecedy, nebo naopak adresáti nejsou uvedeni vůbec.

Další možnosti přináší analýza položek Received: (testy na metody falšování uvedené v kapitole *1.10.2. Způsoby maskování*), spojená například s porovnáním s adresou odesílatele (zpráva vypadá, jako by odešla z některého z freemailů, ale podle hlaviček Received: odešla odjinud, nebo je zpráva podle adresy odeslána například z ČR ale podle IP adresy serveru je odeslána z Číny). Také je možnost porovnávat adresy z položek Received: proti blacklistům. Často se falšují také časy odeslání, které pak nemusí být ani logicky správné (zpráva je například odeslána až po jejím doručení).

Dobré možnosti pro zachycení spamu obsahují také další položky hlavičky, například tyto:

- Identifikace poštovního klienta – je poměrně komplikované rozesílat spam z běžných klientů, spammeři proto používají speciální, nebo se pokoušejí tuto položku v hlavičce falšovat (je třeba odhalit nepřímo).
- Message-ID – z formátu a místa přidání položky Message-ID lze poznat, zda byla zpráva zfalšována, nebo z kterého klienta byla odeslána.
- Předmět obsahuje některé prvky charakteristické pro spam – například text velkými písmeny, text proložený mezerami, velké množství vykřičníků nebo otazníků a podobně.
- V hlavičce jsou obsaženy některé podezřelé položky, jako například X-List-Unsubscribe, Complain-To, X-x a podobně.

Podobně jako u jiných testů i zde mohou negativní testy nebo naopak jiné testy pozitivní (také jejich kombinace) mít zápornou hodnotu, tedy označovat zprávu, která pravděpodobně spamem není.

3.3.7. Software a služby

Pro možnost dosažení rozumné účinnosti s minimálním podílem false positives je nutné výše zmíněné metody obrany proti spamu kombinovat. Běžné mailové klienty/servery mohou podporovat některé z jednodušších metod, ale pro komplexní obranu je třeba většinou použít specializovaný software nebo online služby. Antispamové produkty umožňují technicky provádět velké množství různých filtrů a z jejich výsledků vyhodnotit, zda je zpráva legitimní či nikoliv. Největší devizou jednotlivých produktů však není ani tak množství druhů obsažených filtrů, jako spíše jejich obsah – aby běžný uživatel vytvořil relativně účinnou soustavu filtrů, potřeboval by na to tolik času, že by se tato aktivita rozhodně nevyplatila. Antispamový software však v sobě obsahuje několik stovek předem definovaných filtrů, které si uživatel pouze dolaďuje tak, aby v jeho konkrétních podmínkách byly co nejúčinnější při zachování nízkého poměru false positives. Součástí zakoupeného software také často bývá možnost stahovat si aktualizované filtry, které reagují na změny spamu. Do budoucna se dá také očekávat nárůst významu samoučících algoritmů a využití umělé inteligence.

V testu antispamového software v PC Magazine z února 2003 [26] dosáhly produkty průměrné úspěšnosti od asi 75 % odfiltrovaných spamů u produktů pro jednotlivé uživatele do 85 % u serverových aplikací. Podobně se lišila také pravděpodobnost false positives – zatímco produkty pro jednotlivé uživatele chybně odfiltrovaly jednu legitimní zprávu z dvaceti dvou (4,5 %), u serverových produktů pouze jednu zprávu s pěti set (0,2 %). Dá se však očekávat, že mezi jednotlivými produkty budou také poměrně značné rozdíly.

Filtry, které produkty používají mohou být vytvářeny různými způsoby. Filtry mohou vznikat ručně, kdy firmy získávají vzorky spamových zpráv, vytipovávají charakteristické rysy a podle nich upravují pravidla, nebo strojově, kdy jsou pravidla ze vzorků zpráv vytvářena automaticky (typ pravidel se pro tuto možnost liší, například Brightmail používá jako pravidel jakýchsi „otisků“ zpráv analogických s elektronickým podpisem).

Existuje také několik způsobů, pomocí kterých získávají firmy vzorky zpráv. Mohou je získávat například hlášením od uživatelů (zejména hlášení konkrétních spamů, které prošly kontrolou, může mít velký přínos na efektivní návrh filtrů), nebo provozem vlastní sítě e-mailových adres, které jsou vytvořeny speciálně za účelem být pastí pro spam (*spamtraps*).

Jak již bylo zmíněno v kapitole *3.3.2. Fyzické modely*, můžeme technicky rozdělit produkty na obranu proti spamu do třech skupin:

- produkty působící na straně *klienta*,
- produkty působící na straně *serveru*,
- produkty provozované *externím subjektem*.

Produkty působící na straně klienta jsou většinou určeny pro individuální použití (domácnosti, malé firmy) a vykazují nižší účinnost než produkty působící na serveru, které jsou většinou nasazeny na hromadné použití (velké firmy, instituce, ISP). Produkty provozované externím subjektem nabízejí široké spektrum nasazení spolu s poměrně solidní účinností.

Software většinou používá kombinaci více metod. Jednotlivým testům bývají přiřazeny určité váhy (kladné i záporné) a při překročení určité prahové hodnoty je zpráva označena jako spam. Používány jsou zejména tyto metody:

- analýza klíčových slov v obsahu zprávy,
- analýza formátování zprávy,
- analýza hlaviček zpráv,
- odesílatelé zpráv jsou kontrolováni proti blacklistům,

- uživatelé si mohou vytvářet whitelisty nekontrolovaných odesílatelů/předmětů.

Pokud je zpráva označena jako spam, je provedena například jedna z těchto akcí:

- zpráva je označena v předmětu, hlavičce nebo jinak,
- zpráva je smazána v klientovi/na serveru,
- zpráva je přesunuta do zvláštní složky,
- uživateli je nabídnuta možnost kontaktu spammera nebo ISP (software mohou obsahovat nástroje, které se pokouší vypátrat kontakt na původce zprávy resp. ISP, a nabízejí předpřipravené vzory zpráv).

Následující odstavce obsahují popis některých zajímavých antispamových produktů. Výčet si zdaleka nedělá ambice být úplným (počet existujících produktů by se dal počítat minimálně na stovky), spíše poukazuje na některé cesty, kterými by se vývoj antispamového software a služeb mohl ubírat. Odvětví zatím ještě není ustálené a proto se objevuje velké množství přístupů k problému, které srovnání dále znemožňují. Bude proto zajímavé sledovat, kterými směry se nakonec vývoj vydá nyní, když si problematiku spamu začínají uvědomovat velké firmy, zejména ty již dříve zaměřené na bezpečnost (McAfee, Symantec a podobně).

Velice zajímavý přístup k filtrování spamu nabízí e-mailový klient prohlížeče Mozilla. Mozilla používá bayesiánské filtrování – uživatel musí nejprve klienta naučit, jak vypadá spamová zpráva tím, že spamy označí jako spam. Klient si vytváří slovník slov použitých ve zprávách a přiřazuje k nim hodnoty pravděpodobností, s jakou se vyskytují ve spamech. Podle nich pak kontroluje příchozí zprávy, tak že vypočítává pravděpodobnost pro celou zprávu. Překročí-li pravděpodobnost určitou prahovou hodnotu, je zpráva označena jako spam. Pokud však byla označena legitimní zpráva, může ji uživatel označit jako legitimní, čímž opět dojde k přizpůsobení pravděpodobností. Paul Graham, autor myšlenky využití bayesiánského filtrování pro identifikaci spamu tvrdí [27], že se dá touto metodou realisticky dosáhnout účinnosti 99,5 % s prakticky nulovým množstvím false positives. Na podobném principu pracuje také například SpamProbe (*http://spamprobe.sourceforge.net/*), open-source software pro použití na UNIXových systémech.

Typickým představitelem online služeb je N-Dream‘s Anti-Spam Service (*http://spam.n-dream.com/*). Uživatel si vytvoří na tomto serveru zdarma účet (většina služeb ale bývá komerčních) a zadá přístupové informace do svých schránek (jméno a heslo pro připojení protokolem POP3). Služba se pak každých pět minut připojí do jeho schránky, stáhne všechny zprávy, zanalyzuje je a ty, které považuje za spam, smaže (s tím, že ponechává posledních 100 smazaných spamů jako zálohu pro případ false positives). Základní informace o smazaných zprávách dostává uživatel pomocí e-mailu. Customizace filtrů není možná, jediný způsob, jak může uživatel kontrolu ovlivnit, je zařazení odesílatele do whitelistu.

Alternativu k využívání jednorázových nebo alternativních adres představuje služba Despammed.com (*http://www.despammed.com/*). Uživatel si vytvoří e-mailovou adresu (něco@despammed.com). Zprávy došlé na tuto adresu jsou zkontrolovány pomocí vestavěných filtrů a přeposlány na adresu, kterou uživatel specifikuje. Bohužel tato služba neumožňuje vůbec žádné úpravy, existuje tak poměrně značné riziko false positives. Vzhledem k využití pouze pro rizikové účely to však může stačit.

Cruelmail.com je freemailová služba, která umožňuje vytvářet whitelisty. Uživatel si může prohlížet i zprávy od odesílatelů mimo whitelist a do whitelistu je přidat. Rozdíl proti jiným službám je v tom, že odesílatelé mohou posílat zprávy, které projdou přímo do schránky uživatele, pokud za ně zaplatí částku, kterou si uživatel určí. Služba je zdarma, provozovatel si pouze nechává část z „poštovného.“

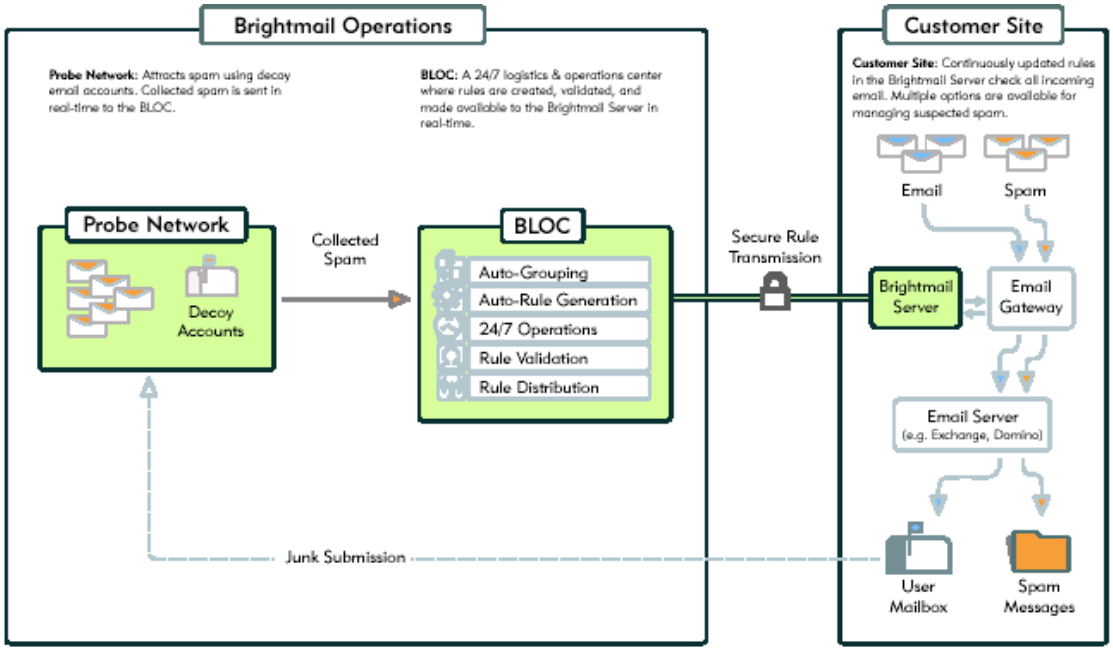
Přístup, který umožňuje obranu nejen proti běžnému spamu, ale také proti ostatním hromadným zprávám, zvolila firma Herbivore (*http://www.herbivore.us/*). Uživatel si nainstaluje platformně nezávislou aplikaci v Javě, která funguje jako proxy mezi libovolným klientem a serverem. Při stažení pošty aplikace nejprve odstraní některé části zprávy tak, aby zůstalo pouze „jádro," vytvoří otisk zprávy a odešle jej na server služby Herbivore. Pokud se stejný otisk vyskytuje vícekrát, jde o hromadnou zprávu a tak není předána klientovi nebo je před předáním označena. Uživatel může ovlivnit její další osud přímo v aplikaci. Systém je doplněn možností používání whitelistů a filtrů a je komerční.

Za jeden z nejúčinnějších serverových nástrojů je považován SpamAssassin. SpamAssassin je perlový skript distribuovaný zdarma, který dokáže identifikovat a označit spamové zprávy pomocí těchto nástrojů:

- Analýza hlaviček a
- analýza textu zprávy – SpamAssassin obsahuje velké množství předdefinovaných filtrů.
- Veřejné blacklisty – SpamAssassin umožňuje porovnávat odesílatele zprávy s mnoha blacklisty včetně MAPS nebo ORDB.
- Razor – Razor je kolaborativní databáze otisků spamových zpráv.

Jednotlivé testy mají určitou hodnotu (kladnou nebo zápornou) a při překročení prahového součtu je zpráva označena jako spam. Systém je dimenzován tak, aby se dal propojit s co nejširším spektrem serverů a tak pro většinu nejběžnějších serverů již existuje konkrétní verze (včetně verze fungující na lokálním stroji jak proxy mezi serverem a klientem). Donedávna existovala také komerční verze pro práci na klientovi nazvaná SpamAssassin Pro, ale po pohlcení firmy Deersoft firmou McAfee byla stažena z prodeje s tím, že algoritmy budou obsaženy v nové verzi software SpamKiller.

Na principu otisků zpráv funguje také software firmy Brightmail (*http://www.brightmail.com/*). Zajímavý je postup, kterým jsou otisky zpráv získávány a distribuovány. Brightmail provozuje několik set tisíc e-mailových účtů, které jsou úmyslně prozrazovány tak, aby přijímaly co nejvíce pošty (na obrázku 2 označeno jako Probe Network). operačním centru BLOC jsou pak z těchto zpráv vytvářeny otisky a pravidla, které jsou přenášeny na server na straně klienta. Klienti mohou zprávy, které kontrolou projdou, poslat zpět do Brightmailu, aby z nich mohl být vytvořen otisk. Brightmail uvádí pravděpodobnost false positives jako pouhou jednu zprávu z miliónu.



Obrázek 2 – Architektura systému Brightmail

3.4. Reaktivní opatření

Reaktivní opatření mají za cíl snížit budoucí dopady spamu reakcí na příchozí spam. Základním opatřením by mělo být smazání zprávy, ideálně ještě před jejím otevřením (pokud je uživatel schopen z adresy odesílatele a předmětu rozpoznat, že jde o spam). Tímto se uvolní místo, které zabírá příchozí pošta a zároveň se minimalizuje možnost napadení virem obsaženým ve zprávě. Problémem může být, že některé mailové klienty zprávu otevírají automaticky (resp. náhled na ni) už při jejím označení, proto nemusí být možnost virového napadení úplně vyloučena.

Pokud je při připojení uživatele aplikována tarifikace podle množství stažených dat (to znamená nejen podle množství skutečných dat, ale také podle času při omezené kapacitě linky), může se dosáhnout značných úspor, když si uživatel nejprve stáhne pouze hlavičky zpráv, spamové zprávy smaže na poštovním serveru a teprve poté stáhne kompletní zprávy.

Důležitou součástí reaktivních opatření je reportování zpráv, které projdou sítem dynamických opatření, zodpovědné osobě (typicky správci pošty) tak, aby mohly sloužit k přenastavení filtrů a pravidel a případně i ke stížnostem nebo právním akcím. Nejjednodušším způsobem hlášení je přeposílání spamu (nejlépe na vyhrazenou adresu), sofistikovanější možnosti mohou obsahovat například mailové klienty – stisknutím tlačítka nebo klepnutím na odkaz je zpráva označena jako spam a předána zodpovědné osobě.

Další možnosti skýtají aktivní akce – *kontaktování spammera nebo jeho ISP*. Toto již vyžaduje poměrně značnou energii a tak se dá využití omezit pouze na relativně malé množství zpráv. Přímé kontaktování spammera může být poměrně účinnou metodou, ale naopak může být naprosto kontraproduktivní a přinést podstatný nárůst v objemu spamu. Většina spamů obsahuje odkaz nebo návod na možnost vyřazení ze seznamu spammera. Někdy jde o zaslání e-mailu na určitou adresu (často s určitým klíčovým slovem v předmětu nebo textu zprávy), někdy jde o načtení webové stránky nebo o zadání e-mailové adresy do formuláře. Tato možnost může stejně jako k vyřazení adresy ze seznamu sloužit i k ověření toho, zda je adresa funkční, zda zprávy poslané na tuto adresu uživatel čte a tak i ke zvýšení ceny této adresy.

Podobná situace platí pro zasílání zpráv spammerovi – pokud spammer neuvedl odkaz na odstranění ze seznamu, je pravděpodobné, že na zaslanou zprávu nebude adekvátně reagovat. V některých případech (zejména u menších spammerů, například v ČR) sice může přímý

kontakt vést k vyřazení z databáze, v každém případě si spammer ověří, že daná adresa je funkční. Záleží tedy pouze na přístupu spammera. Další problém zde vnáší časté maskování stop – kontaktovat spammera tak nemusí být vůbec jednoduché. Adresa odesílatele bývá velice často zfalšovaná nebo již není funkční (v případě jednorázových adres), může dokonce patřit někomu, kdo s rozesíláním spamu nemá vůbec nic společného. Identitu spammera je také možné zjistit pomocí hlavičky zprávy (pole Received:, viz *1.10.2. Způsoby maskování*) a zjištění kontaktních údajů v adresáři vlastníků domén.

Jiným druhem zasílání zpráv spammerovi je tzv. *fake bouncing* – zasílání falešných zpráv o nedoručitelnosti zprávy. Poté, co je spam adresátem nebo automaticky identifikován, je zpět odeslána zpráva o tom, že spam nebyl doručen s vírou, že spammer adresu vyřadí ze seznamu. Vzhledem k tomu, že adresy odesílatelů bývají často falšovány, je účinnost této metody diskutabilní, spammeři se navíc budou řídit spíše tím, že poštovní server v SMTP komunikaci potvrdil přijetí pro korektního uživatele.

Také nákup produktů, konkrétně software, který je inzerován pomocí spamu, může být riskantní záležitostí – pokud není jeho tvůrci proti mysli inzerovat svůj produkt nemorálním způsobem, existuje zde velká pravděpodobnost, že mu nebude proti mysli do software zabudovat například zadní vrátka nebo procedury pro odesílání zjištěných údajů (kterými může například být obsah adresáře – spammer tak má hned několik desítek ověřených adres k dobru).

Větší efekt může přinést kontakt ISP, z jehož serverů byla zpráva odeslána. Adresa serveru se dá opět zjistit z hlavičky zprávy, konkrétně z druhé nejnižší položky Received:. Z této adresy je možné (například pomocí služby WHOIS) získat doménové jméno, případně také kontaktní údaje (adresy správců a podobně). Pokud je známé pouze doménové jméno, je možné vyzkoušet některou ze standardních adres, jako je například abuse@doména.tld, postmaster@doména.tld nebo root@doména.tld. Vzhledem k tomu, že odpovídání na stížnosti uživatelů je pro ISP poměrně nákladné, existuje zde poměrně dobrá šance, že ISP proti spammerovi zakročí. Avšak i zde může v případě, že ISP je jakýmsi způsobem se spammerem propojen, nastat situace, kdy pouze dojde k ověření adresy a tak je efekt záporný. Dá se ale očekávat, že pravděpodobnost tohoto jevu je nižší, než u kontaktu se spammerem. Kontaktování spammera nebo jeho ISP mohou usnadnit některé softwarové produkty nebo online služby jako například Spamcop.net (*http://www.spamcop.net*).

Zajímavou možnost reaktivního opatření nastiňuje sloupek Seana Gallaghera [28]. Nejde však o opatření pro budoucí zamezení přijímání zpráv jako spíše o určitý druh pomsty spammerovi – spamback. Podstatou spambacku je generování fiktivních zájemců o inzerovaný produkt zadáváním falešných kontaktních údajů na stránky spammera. Tím by spammerům vzrostly náklady na vyřazení neplatných údajů resp. vyhledávání skutečných zájemců a mohlo by tak dojít k tomu, že ekonomická výhodnost spammingu se nejen sníží, ale také přesune do záporných čísel. Po úspěch by však bylo nutné masivní nasazení, které je však nepravděpodobné.

Jiný přístup nabízí nezisková organizace Remove.org (*http://www.remove.org/*), která udržuje seznam uživatelů internetu, kteří si nepřejí být kontaktováni spammery. Za členství musí uživatel platit necelých deset dolarů za rok, za které získává zařazení do seznamu a kompletní agendu vyřizování stížností nebo právních sporů v případě nerespektování rozhodnutí uživatele nepřijímat spam. Organizace však neuvádí jaká je účinnost jejich počínání.

3.4.1. Právo

V poslední době začínají na rostoucí problém se spamem reagovat také státy vydáváním specializovaných zákonů nebo úpravou zákonů stávajících, které regulují pravidla elektronické reklamy a umožňují tak spammery trestně stíhat. Bohužel problém není tak jednoduchý jak se zdá, neboť:

- náklady spojené s právní akcí proti každému spammerovi, od kterého dostane uživatel zprávu, několikanásobně převyšují náklady způsobené spamem,
- vypátrat identitu spammera nemusí být úplně snadné,
- mohou nastat problémy s dokazováním,
- obrana je komplikována efektivností právního systému a obecně vymahatelností práva,
- spamming není jev omezený na jeden stát (jednu jurisdikci), proto může být právní akce ještě komplikována mezinárodním právem.

Zatímco v České republice není prakticky možné vysoudit od spammera náhradu škody nebo jinou kompenzaci, například v některých státech v USA je zákonem dána minimální výše odškodného za došlou nevyžádanou zprávu. Například ve státě Washington tato kompenzace činí 500 dolarů, což znamená nejen poměrně značný trest pro spammera, ale také motivaci proti spammerovi bojovat.

To, že byly zákony zabývající se spamem v národních (a nadnárodních) parlamentech přijaty, je často zásluhou nátlakových (lobbyistických) organizací. Například direktiva v Evropské unii (viz *3.4.1.2. Evropská unie*) byla velice ovlivněna organizací EuroCAUCE (The European Coalition Against Unsolicited Commercial Email) – dobrovolnou organizací evropských uživatelů internetu, odborníků a ISP. Podobně existují organizace jako CAUCE (ve Spojených státech amerických), CAUCE Canada, CAUCE India nebo CAUCE AU v Austrálii, všechny zahrnuty do iCAUCE (International CAUCE), mezinárodní koalice proti nevyžádané komerční poště.

Samozřejmě, že se proti zavádění antispamových zákonů ozývají i spammeři, naštěstí jsou ve většině případů zákonodárci nakloněni spíše uživatelům.

3.4.1.1. Česká republika

V České republice se spammingu dotýkají dva zákony – zákon o regulaci reklamy (138/2002 Sb., přesněji zákonem 40/1995 Sb. ve znění pozdějších předpisů) a částečně také zákon o ochraně osobních údajů (101/2000 Sb.). Zákon o regulaci reklamy obsahuje tuto formulaci:

> § 2
> (1) Zakazuje se
> …
> e) šíření nevyžádané reklamy, pokud vede k výdajům adresáta nebo pokud adresáta obtěžuje.

Podle této formulace je zřejmé, že spam se dá považovat za zakázaný druh reklamy, neboť vede k výdajům adresáta (minimálně výdaje za přenos dat) a může jej také obtěžovat.

O tom, že tato zákonná úprava je v boji proti spamu alespoň částečně účinná, přesvědčila „kauza Tvujdum.cz“. Podstatou bylo rozeslání několika desítek tisíc mailů na adresy po českém internetu, tedy akce v ČR bezprecedentní. Veřejnost se postavila negativně a po iniciativě vedené zejména serverem Pooh.cz a dalšími bylo zasláno několik desítek podání k živnostenskému odboru zodpovědného krajského úřadu (toto podání je jako vzor uvedeno v příloze 1), nakonec byl spammer postižen pokutou ve výši „několika desítek tisíc korun“ [29].

Podle zákona o regulaci reklamy tedy možnost obrany existuje podáním k živnostenskému odboru krajského úřadu.

Také zákon o ochraně osobních údajů (101/2000 Sb.) poskytuje určité možnosti obrany proti spamu. Podle stanoviska Úřadu pro ochranu osobních údajů k monitorování elektronické pošty a ochraně soukromí a osobních údajů zaměstnanců [30] je e-mailová adresa, která obsahuje

jméno a příjmení, osobním údajem a zákon se tak na její ochranu vztahuje. Proti spammerovi je tak možné zakročit v případech:

- kdy adresa obsahuje jméno a příjmení uživatele a zároveň
- adresa nebyla dříve zveřejněna (byla získána z neveřejných zdrojů) nebo
- spammer neměl souhlas s jejím zpracováním nebo
- byla v hlavičce mailu uvedená spolu s dalšími adresami (takže ji mohli získat jiní uživatelé).

Stížnosti na porušení zákona o ochraně osobních údajů řeší Úřad pro ochranu osobních údajů.

3.4.1.2. Evropská unie

Vzhledem k tomu, že by se Česká republika měla brzy stát členskou zemí Evropské unie, je zajímavé se podívat na to, jak problematiku spamu řeší její právní systém. Direktiva o ochraně dat v komunikaci (Communications Data Protection Directive, 2002/58/EC, [31]), která byla schválena Evropskou komisí v prosinci 2002 a v členských zemích by měl být implementován počátkem listopadu 2003, se spamem zabývá poměrně podrobně.

Nejdůležitější je pravděpodobně článek 40, který zakotvuje tzv. opt-in – pokud chce někdo zasílat reklamní zprávy (a to nejen elektronickou poštou, ale také telefonem, faxem nebo SMS zprávami), musí mít explicitní souhlas uživatele. Článek 41 upravuje používání kontaktních údajů z již existujících vztahů pro direct marketing – aby mohly být tyto údaje používány, musí o tom být případný adresát informován a musí mít možnost toto odmítnout. Tedy například při registraci software musí být uživatel informován o tom, že bude jednou měsíčně dostávat novinky o nových verzích, a musí mít možnost toto odmítnout, tato možnost se navíc musí opakovat s každým oslovením. V článku 43 je také ustanoven zákaz používání falešných identit a falešných adres pro odpověď.

Direktiva Evropské unie tedy poměrně značně omezuje možnosti spammerů, problémem však zůstává to, že drtivá většina spamu je rozesílána ze zemí mimo EU, což možnosti právní obrany značně ztěžuje.

3.5. Závěr kapitoly

V této kapitole byly definovány tři druhy opatření proti spamu: preventivní, dynamická a reaktivní. Klíčem k prevenci proti spamu je zamezení dostupnosti adresy pro spammera. Jako nejčastější prostředky jsou zmiňovány využívání sekundárních nebo jednorázových adres, maskování adres, využívání formulářů, dodržování pravidel elektronické pošty a vhodná volba formátu e-mailových adres.

Existuje velké množství dynamických opatření mezi které patří například filtrování zpráv podle odesílatelů (blacklist nebo whitelist), podle klíčových slov v obsahu zprávy, podle formátování zprávy, podle položek hlavičky zprávy a podobně. Využívání jednoduchých možností obrany umožňuje většina standardních produktů (poštovních serverů a klientů), pro větší úspěšnost je však nutné použít některý ze specializovaných produktů (software nebo online služeb).

Reaktivní opatření zahrnují odhlášení ze seznamů spammera, mazání zpráv, reportování spamu, kontakt spammera nebo jeho ISP a možnosti právní obrany. Právní obrana není jednoduchým řešením, většina civilizovaných zemí však jakýmsi způsobem spam právně reguluje. V České republice se spamu týkají dva zákony – zákon o regulaci reklamy a zákon o ochraně osobních údajů. V Evropské unii je právě zaváděna direktiva o ochraně dat v komunikaci, která zavádí mimo jiné tzv. opt-in.

4. Postup vedoucí k minimalizaci nákladů

4.1. Úvod kapitoly

Tato kapitola se pokouší alespoň nastínit některé prvky postupu vedoucího k minimalizaci nákladů způsobených spamem na straně příjemce. Na začátku jsou zmíněna východiska postupu: několik průzkumů postojů uživatelů včetně výsledků dotazníkového šetření provedeného speciálně pro tuto diplomovou práci.

Doporučený postup je vytvořen na základě využívaných metodologií informační bezpečnosti. Kapitola obsahuje stručný úvod do informační bezpečnosti (se zaměřením na obranu proti spamu), v další části se práce zabývá risk managementem a zejména procesem výběru protiopatření.

4.2. Východiska

4.2.1. Průzkum CDT

V březnu 2003 byly CDT (The Center for Democracy and Technology) zveřejněny výsledky šestiměsíčního průzkumu chování spammerů [32]. Princip průzkumu byl jednoduchý – CDT vytvořilo během léta 2002 asi 250 e-mailových adres, každou z nich jednou použilo pro některou z rizikových aktivit, a zkoumalo, které z adres přitáhly spammery a jaký objem spamu na ně byl odesílán. Adresy měly podobu náhodného řetězce, aby nehrozila možnost, že na ně spammer přijde náhodou a byly zveřejněny těmito cestami (pro každou bylo použito několik způsobů zveřejnění):

- *Webové stránky* – adresy byly zveřejněny běžnou cestou nebo maskovány (obrázek, HTML entity), některé odstraněny po dvou týdnech.
- *USENET* – některé adresy zveřejněny v hlavičce, některé v textu (z toho část maskována).
- *Webové služby* – adresy byly zadány do některé z online služeb, po dvou týdnech nebo po přijetí zprávy některé z nich odhlášeny ze zasílání zpráv.
- Zveřejnění ve *webových diskusích* a podobně – adresy zveřejněny na diskusních serverech, aukcích nebo serverech s nabídkou práce (opět některé maskovány).
- Databáze *WHOIS* – zveřejněny jako část registrace domén .com nebo .org.

Během šesti měsíců bylo dohromady přijato zhruba deset tisíc zpráv, z nichž asi 1600 tvořily legitimní zprávy (z online služeb), 62 zpráv bylo neklasifikovatelných (chybějící data), šestnáct zpráv bylo přijato během dvou týdnů po odhlášení ze zasílání zpráv (což použitá metodologie považovala za legitimní) a zbývajících 8842 zpráv byly spamy. Podle zdroje získání adresy byly zprávy rozděleny takto:

- 8609 zpráv – zveřejnění na webových stránkách
- 110 zpráv – zveřejnění na USENETu
- 82 zpráv – obdrženo po odhlášení ze zasílání zpráv
- 25 zpráv – neschválené sdílení nebo prodej e-mailových adres webovými službami
- 15 zpráv – adresy zveřejněny na diskusních skupinách
- 1 zpráva – adresa byla použita při registraci domény

Množství zpráv došlých na adresy zveřejněné na webových stránkách záviselo zejména na dvou faktorech: známosti stránek, kde byly zveřejněny (jejich zařazení do vyhledávačů a podobně), a době zveřejnění (adresy zveřejněné pouze na dva týdny dostávaly podstatně menší množství zpráv. Na adresy, u kterých bylo použito maskování, nepřišla ani jedna zpráva. Adresy, které byly po dvou týdnech odstraněny, vykazovaly po odstranění signifikantní klesající tendenci ve srovnání s kontrolními adresami zveřejněnými po celou dobu průzkumu.

Podobná situace panovala také u adres zveřejněných na USENETu. Množství zpráv záviselo na skupině, ve které byly zveřejněny (nejvíce zpráv dostala adresa zveřejněná ve skupině alt.sex.erotica). Jen jedno procento zpráv připadalo na adresy zveřejněné v textu zprávy (zbytek na zveřejnění v hlavičce), na maskované adresy nepřišlo opět nic.

Další část průzkumu byla zaměřena na to, jak společností respektují preference uživatelů. E-mailové adresy zadané do online služeb byly po určité době odhlášeny z rozesílání zpráv. Z 31 webových služeb 26 respektovalo preference a přestalo na adresy zasílat zprávy. Pět služeb však rozesílalo zprávy dále (celkem 82 zpráv).

Diskuse (s patnácti zprávami na adresu z pouze jedné diskuse) a registrace domén (pouze jedna zpráva) se ukázaly jako relativně bezpečné způsoby zveřejnění adres.

Průzkum se také zabýval rizikem útoků na poštovní servery, kdy je na servery rozesíláno velké množství zpráv na adresy, které obsahují jako jméno příjemce náhodnou kombinaci písmen nebo slovníková hesla. Jeden ze sledovaných serverů tak obdržel 8506 zpráv (než byl nastaven filtr) na generované adresy jako například:

```
a@egovtoolkit.org
b@egovtoolkit.org
c@egovtoolkit.org
d@egovtoolkit.org
…
z@egovtoolkit.org
aa@egovtoolkit.org
ab@egovtoolkit.org
ac@egovtoolkit.org
ad@egovtoolkit.org
…
zz@egovtoolkit.org
aaa@egovtoolkit.org
aab@egovtoolkit.org
aac@egovtoolkit.org
aad@egovtoolkit.org
…
zzz@egovtoolkit.org
aaaa@egovtoolkit.org
aaab@egovtoolkit.org
aaac@egovtoolkit.org
```

Během trvání průzkumu byl také na jeden ze serverů proveden útok pomocí slovníkových hesel, výsledná čísla bohužel nejsou v průzkumu uvedena.

Zpráva o průzkumu shrnuje závěry do osmi bodů:

- E-mailové adresy zveřejněné na webu jsou spammery často používány.
- Množství spamu poslaného na adresu zveřejněnou na webu je přímo úměrné návštěvnosti webových stránek, kde byla adresa zveřejněna.

- E-mailové adresy získané z webu jsou používány relativně krátce (po odstranění adres množství přijatých zpráv klesá).
- Zveřejnění adres na USENETu je signifikantním zdrojem, ačkoliv ve srovnání s webem je počet zpráv podstatně nižší.
- Maskování e-mailových adres je efektivním způsobem zamezení získávání adres z webových stránek nebo USENETu.
- Online služby, které publikují podmínky a dávají uživatelům možnost výběru (zda dostávat nebo nedostávat zprávy) tyto podmínky většinou respektují.
- Registry doménových jmen nejsou pro spammery velkým zdrojem adres.
- I když nebyla adresa nikde zveřejněna, je možné dostávat spamové zprávy skrz útoky na poštovní server.

4.2.2. Průzkum Federal Trade Commision

Průzkum Federal Trade Commision (vládní komise v USA, která se zabývá antitrustovými zákony a zákony na obranu spotřebitelů) byl zaměřen na pravdivost informací obsažených ve spamu [33]. Podle této studie provedené na vzorku tisíce zpráv obsahuje většina spamu lživá tvrzení; informace o obchodních příležitostech a investicích jsou zavádějící až v 96 %.

Obchodní příležitosti, frančízink, práce z domova tvořily asi 20 % zpráv, 18 % pornografie nebo seznamky a 17 % pojištění, nabídky kreditních karet a podobně. U třetiny zpráv byl zfalšován odesílatel, v polovině případů se zprávy snažily předstírat, že příjemce odesílatele zná.

4.2.3. Průzkum společnosti Symantec

Průkopník online průzkumu trhu společnost InsightExpress provedla pro Symantec Inc na podzim roku 2002 průzkum na vzorku tisíce uživatelů zaměřený zejména na postoje veřejnosti ke spamu obecně a k vážnosti situace [34].

Podle průzkumu dostává 37 % respondentů týdně více než 100 nevyžádaných zpráv, 60 % více než 50 zpráv. 69 % respondentů souhlasilo, že nevyžádaná pošta uživatelům elektronické pošty většinou škodí. 77 % dotazovaných s dětmi do osmnácti let uvedlo, že mají obavy, že jejich děti mohou číst nevyžádanou poštu.

84% respondentů souhlasilo, že je nevyžádaná pošta připravuje o jejich osobní čas; 65 % resp. 24 % uvedlo, že nad nevyžádanou poštou tráví denně více než 10 resp. 20 minut.

Jako největší problémy spojené s nevyžádanou poštou byly vyhodnoceny:

- 38 % – pornografický nebo jinak nevhodný obsah,
- 36 % – ztráta času spojená s odstraněním nebo odhlášením nevyžádané pošty,
- 18 % – odčerpávání omezených zdrojů počítače a elektronické pošty,
- 18 % – obtížnost odhlašování a blokování nevyžádaných zpráv,
- 18 % – samotná nevyžádanost a nevítanost zpráv.

74 % respondentů vnímá, že se objem nevyžádané pošty zvyšuje, naopak 4% uvedla, že se objem snižuje. 42 % dotazovaných nepoužívá filtr nevyžádané pošty i když souhlasí s tím, že je spam problémem.

4.2.4. Průzkum Survey.net

Webové stránky Survey.net se specializují na online průzkumy. Od července 1997 běží online průzkum s názvem Internet Spam/UCE (Unsolicited Commercial E-mail) #1 [35], do dnešního dne na něj odpovědělo 4337 respondentů. Vzhledem k tomu, jak dlouho průzkum probíhá, se dá očekávat, že spíše než současný stav bude v průzkumu zachycen jakýsi průměr a některé z odpovědí tak již na první pohled vypadají neaktuální. V každém případě podle tohoto průzkumu považuje skoro 52 % respondentů spam za velmi obtěžující (27 % obtěžující), zatímco pouhých 3,3 % dotazovaných má spam rádo. Jako ideální prostředek pro regulaci spamu je zde uváděno povolení spamu s tím, že každá zpráva bude označena.

4.2.5. Průzkum SurfControl

Na přelomu let 2002 a 2003 provedla kalifornská firma SurfControl dva průzkumy [36] na zhruba 1400 a 1000 IT profesionálů zaměřené na legislativní kontrolu spamu. Devět z deseti dotazovaných podporovalo snahu zavést tvrdá legislativní opatření proti spamu, regulaci pornografického spamu a tresty za lživé nebo zavádějící informace obsažené ve spamových zprávách. Zároveň však 68% respondentů věří, že samotná legislativa bez podpory technologií problém nevyřeší. Pouze 56% dotazovaných udává, že jejich zaměstnavatel používá antispamové systémy.

4.3. Vlastní dotazníkové šetření

Jako jedno z východisek pro vytvoření metodiky byl zvolen průzkum zkušeností uživatelů elektronické pošty s prostředky obrany proti spamu. Hlavním cílem bylo získat dostatečné množství relevantních dat pro nalezení odpovědí na tyto otázky:

- Jaký problém pro uživatele spam představuje – objektivně (počty zpráv) i subjektivně (jak uživatelé spam vnímají)?
- Jaké metody obrany proti spamu jsou používány?
- Jaká je úspěšnost jednotlivých metod v obraně proti spamu?

4.3.1. Popis použité metody

4.3.1.1. Odůvodnění podoby dotazníku

Pro sběr dat byla zvolena metoda dotazníkového šetření. Dotazník byl navrhován tak, aby korespondoval se strukturou této práce, konkrétně s částí *Analýza dostupných možností obrany*. Otázky proto byly rozděleny do šesti graficky oddělených bloků:

- Základní informace,
- Prevence,
- Blokování,
- Software,
- Přímý kontakt,
- Právo.

Každý blok obsahuje několik otázek týkajících se zejména konkrétního chování respondenta (např. zda filtruje elektronickou poštu) a je ukončen otázkou, která na pětibodové škále (rozhodně ano, spíše ano, nevím, spíše ne, rozhodně ne) zjišťuje postoj k danému tématu. Každá

otázka byla také doplněna krátkým vysvětlujícím textem. Typ otázky byl volen podle charakteru odpovědí – byly použity tyto typy otázek:

- výběr jedné možnosti (v dalším textu označeno jako „1“),
- výběr více možností („n“),
- zadání konkrétní číselné hodnoty („x“),
- u některých otázek bylo součástí také doplňující pole, které umožnilo respondentovi odpovědět i jinou, než nabízenou odpovědí („d“).

Cílem bloku *Základní informace* bylo zjistit základní informace o respondentovi a jeho postoji ke spamu. První otázka (Jaká je vaše pozice?, 1) sloužila k rozdělení respondentů do segmentů pro přesnější analýzu (viz kapitola *4.3.1.3. Výběr, segmentace a oslovení respondentů*). Následující série třech otázek (Kolik poštovních schránek spravujete?, x; Kolik e-mailových zpráv denně dostáváte?, x; Jaký podíl z těchto mailů tvoří spam?, 1) zjišťovala absolutní čísla o objemu zpráv a podílu spamu. Další otázka (Jste si vědom, odkud získal spammer vaši e-mailovou adresu?, n) testovala, zda si jsou respondenti vědomi odkud byla získána jejich adresa a také k identifikaci nejčastějších způsobů získávání adres. Poslední dvě otázky zjišťovaly postoj uživatelů ke spamu z pohledu aktivita/pasivita v obraně (Bráníte se aktivně proti spamu?, 1) a z pohledu vážnosti situace (Považujete spam za vážný problém?, 1).

Blok *Prevence* obsahoval otázky týkající se vyhýbání se spamu (viz kapitola *3.2. Preventivní opatření*). První otázka (Máte k dispozici rady jak se vyhnout spamu a jak s ním zacházet?, n) zjišťovala jak moc jsou uživatelé elektronické pošty informováni o prevenci spamu. Následující otázka (Používáte pro riskantní situace zvláštní e-mailovou adresu?, 1) pomáhala odhadnout, jak moc uživatelé využívají rozdělení adres podle stupně bezpečnosti. Poslední otázka zjišťovala odhadovanou účinnost prevence (Považujete prevenci spamu za dostatečně účinný prostředek?, 1).

V bloku nazvaném *Blokování* byl zjišťován přístup respondentů k eliminaci podezřelých e-mailů podle různých kritérií (viz kapitola *3.3.1. Filtrování zpráv*) – podle klíčových slov (Filtrujete e-maily podle klíčových slov?, 1), nebo podle původu zprávy (Blokujete poštu od jiných než povolených uživatelů?, 1; Blokujete poštu od konkrétních uživatelů/z konkrétních serverů?, nd). Na závěr byl opět zjišťován postoj k účinnosti těchto metod (Považujete blokování spamu za dostatečně účinný prostředek?, 1).

Další blok zkoumal možnosti využití speciálního *Software* (viz kapitola *3.3.7. Software a služby*). První otázka zjišťovala zda respondent využívá software a v jaké podobě (Používáte nějaký software na obranu proti spamu?, n). Dále jsem se pokusil identifikovat konkrétní softwarové produkty (Který software na obranu proti spamu používáte?, nd) – respondent měl na výběr z pěti známých produktů, mohl doplnit další. Blok ukončovala otázka zjišťující postoj k účinnosti software (Považujete software za dostatečně účinný prostředek?, 1).

Blok *Přímý kontakt* byl zaměřen na kontakt poškozeného se spammerem nebo poskytovatelem jeho připojení (viz kapitola *3.4. Reaktivní opatření*) a úspěšnost tohoto počínání (Snažil jste se někdy kontaktovat spammera?, 1; Snažil jste se někdy kontaktovat poskytovatele připojení/správce pošty serveru, odkud vám přišel spam?, 1) a na účinnost přímého kontaktu (Myslíte si, že má smysl kontaktovat spammera/jeho ISP?; 1).

Poslední blok nazvaný *Právo* zkoumal možnosti právní cesty obrany proti spammingu (viz kapitola *3.4.1. Právo*). První otázka se zaměřovala na zkušenosti respondentů (Snažil jste se někdy bojovat proti spammerovi právní cestou?, 1), druhá otázka zjišťovala účinnost právní obrany (Myslíte si, že je současné právo dostatečně účinné v boji proti spamu?, 1).

Dotazník byl doplněn textovým polem, do kterého mohli respondenti zadat své připomínky k dotazníku nebo k tématu (které se v dalším průběhu tvorby diplomové práce ukázaly být

velice podnětné). Ti respondenti, kteří zadali také e-mailovou adresu, byli o výsledcích průzkumu informováni elektronickou poštou.

Celý dotazník včetně všech odpovědí a úvodního textu se nachází v příloze 2.

4.3.1.2. Technické provedení

Jako nejvhodnější forma pro dotazník byla vyhodnocena forma webového formuláře, který ukládá data do databáze, a to zejména z těchto důvodů:

- jednoduché zadání údajů uživatelem,
- stálý přehled o aktuálním stavu šetření,
- možnost analýzy dat pomocí přímých dotazů na databázi,
- snadný přenos dat do dalších analytických nástrojů.

Vzhledem ke zkušenostem a snadné dostupnosti byla zvolena kombinace jazyka PHP, databáze MySQL a školního linuxového serveru Sorry. Jako uživatelské rozhraní byla zvolena stránka v jazyce HTML, zejména formulářové prvky tohoto jazyka (FORM, INPUT, SELECT a podobně). Uživatel požádá server o provedení skriptu index.php, který nejprve zobrazí zmíněný formulář. Po vyplnění formuláře uživatel stiskne tlačítko pro odeslání. Pomocí JavaScriptové funkce je provedena kontrola správnosti zadání číselných údajů a data jsou následně metodou POST (odesílaná data nejsou součástí URL, ale součástí HTTP žádosti) předána zpět skriptu index.php, který je uloží do databázové tabulky a informuje uživatele o výsledku, resp. ošetří chybové stavy.

Tabulku, do které se ukládají data, tvořil jeden sloupec pro každou otázku s možností výběru jedné odpovědi nebo zadání konkrétní odpovědi a jeden sloupec pro každou odpověď k otázce s možností výběru více odpovědí. Tabulka dále obsahovala sloupec, do kterého byla ukládána IP adresa odesílatele, z důvodu ochrany osobních údajů zakódována algoritmem MD5, pro kontrolu případných duplicitních záznamů. Tabulka byla několikrát týdně zálohována.

Při analýze výsledků bylo použito dvou metod. Některé údaje, zejména četnosti, byly získávány přímo z databáze pomocí SQL dotazů. Celá tabulka pak byla přenesena přes formát CSV do aplikace Microsoft Excel, kde byly prováděny analýzy, které nebylo technicky možné provést na databázi, a kde byly připraveny tabulky a grafy.

Některé z řádků, které obsahovaly podezřelá data (zejména extrémně vysoké hodnoty počtu schránek kombinované s velice nízkými podíly zpráv na schránku a neuvedenou e-mailovou adresou), byly z databáze vyřazeny, aby nebyly těmito extrémy ovlivněny statistiky absolutních počtů.

4.3.1.3. Výběr, segmentace a oslovení respondentů

Před zahájením tvorby dotazníku bylo nutné rozhodnout o výběru a segmentaci respondentů. V úvahu připadaly dva postupy – omezit respondenty na konkrétní segmenty nebo výběr respondentů neomezovat a provádět segmentaci dodatečně otázkou v dotazníku. Zvolena byla nakonec druhá varianta, a to zejména z těchto důvodů:

- dal se očekávat větší počet respondentů, a tak i větší vypovídací schopnost statistik,
- snadnější oslovení respondentů – respondenty lze oslovit plošně (pomocí odkazů na webových stránkách, v diskusních skupinách a podobně); druhá varianta by vyžadovala oslovení přímé,
- dodatečná segmentace uživatelů umožňuje interpretovat data z různých perspektiv (postmaster může mít na věc jiný pohled než běžný uživatel).

Respondenti měli možnost přihlásit se k jednomu z pěti segmentů podle pozice v první otázce dotazníku. Byly zvoleny tyto segmenty:

- *Postmaster* – může poskytnout čistě technologický pohled zaměřený úzce na problematiku pošty.
- *IT manager* – stále technologický pohled, ale již v širším kontextu.
- *Manager* – pohled prizmatem efektivity, produktivity, nákladů a podobně.
- *Uživatel* – pohled běžného uživatele zaměřený zejména na konkrétní problémy (náklady za připojení, vyrušení, nutnost mazat spamy a podobně).
- *Jiná pozice* – pro respondenty, kteří se nechtějí nebo nemohou zařadit do předchozích segmentů.

Protože se otázky daly z různých pozic chápat různě, byly potenciálně sporné otázky upřesněny ve vysvětlujícím textu. Uživatelé, kteří si přáli odpovědět z více pozic, měli možnost odeslat otazník vícekrát. Nebylo povinné odpovídat na všechny otázky, neboť v určitých situacích z některých pozic nemusely dávat smysl, nebo nemohly být pro neodbornou veřejnost srozumitelné.

Oslovení uživatelů probíhalo v několika fázích. V první fázi bylo o dotazníku informováno několik desítek uživatelů pomocí komunitních webových stránek a IM ICQ a Jabber. Několik z nich dotazník vyplnilo a předalo připomínky, na základě kterých byly některé otázky v dotazníku upraveny. Vzhledem ke lhůtám byl odkaz na dotazník zadán do několika internetových vyhledávačů (Seznam, Atlas, Centrum). Jako klíčový nástroj oslovení uživatelů byly zvoleny internetové magazíny pro odbornou veřejnost, které se systematicky zabývají problematikou spamu. Za umístění odkazu jim bylo přislíbeno předání výsledků dotazníkového šetření. Několik magazínů odkaz na své stránky umístilo (viz *4.3.1.4. Harmonogram*), některé dokonce samy od sebe.

4.3.1.4. Harmonogram

27. 2. 2003 – formulář zprovozněn, během prvních několika dní prováděny drobné úpravy na základě zpětné vazby od několika vybraných uživatelů

28. 2. 2003 – přidání odkazu na dotazník do vyhledávačů Seznam, Atlas a Centrum. Odeslán e-mail s žádostí o zveřejnění odkazu na pět českých serverů zabývajících se spamem.

1. 3. 2003 – zobrazení odkazu na serveru Underground.cz, ve vyhledávači Atlas

3. 3. 2003 – odkaz zobrazen na serverech Technet.cz, Lupa.cz, Pooh.cz

5. 3. 2003 – odkaz zobrazen ve vyhledávači Centrum

18. 3. 2003 – odkaz zobrazen na stránkách České společnosti pro systémovou integraci

Na průzkum bylo také průběžně upozorňováno v diskusních skupinách (USENET) a v diskusích k článkům na téma spam na odborných serverech.

16. 4. 2003 – ve večerních hodinách byl dotazník odstraněn

4.3.2. Výsledky šetření

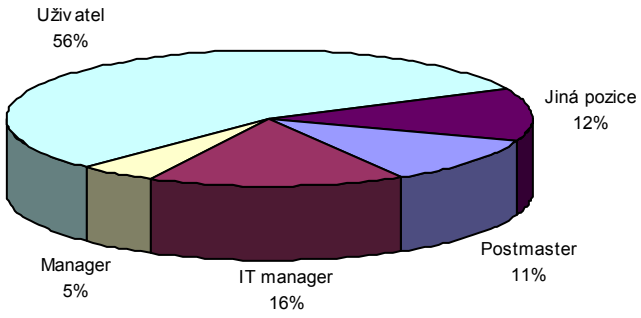
Po skončení průzkumu se v databázi nacházelo 697 řádek, tedy 697 odeslaných dotazníků. Po počáteční analýze byly dva řádky označeny jako velice podezřelé (velmi vysoké počty schránek, které tvořily více než polovinu celkového počtu, při naprosto minimálním počtu zpráv – necelé dvě zprávy na tisíc schránek a den), neobsahovaly e-mailovou adresu, která by umožňovala

údaje ověřit, a proto byly z databáze odstraněny. Dále byly odstraněny další dva řádky, které se ukázaly jako duplicitní. Po vyčištění tedy tabulka obsahovala 693 řádek.

Jeden ze sloupců tabulky obsahoval zakódované IP adresy, které měly sloužit zejména pro kontrolu duplicitních řádek. Dohromady bylo v tomto sloupci 633 unikátních IP adres. Rozdíl mezi celkovým počtem řádek a počtem IP adres se dá vysvětlit tím, že uživatelé měli možnost odesílat dotazník z různých pohledů vícekrát. Nelze však říci, že by to znamenalo přesně 633 respondentů, protože z některých IP adres byly prokazatelně (podle kombinace s uvedenou e-mailovou adresou) odesílány dotazníky více uživatelů. Dá se tedy předpokládat, že celkový počet osob, které na dotazník odpověděly, je necelých 640.

4.3.2.1. Základní informace

Blok nazvaný *základní informace* měl za cíl zjistit základní informace o respondentech a jejich postoji ke spamu. První otázka (Jaká je vaše pozice?) sloužila k segmentaci respondentů. Svou pozici uvedli všichni dotazovaní, rozdělení je zobrazeno v obrázku 3.



Obrázek 3 – Rozdělení segmentů

V absolutních číslech tedy na dotazník odpovědělo 77 postmasterů, 109 IT managerů, 33 managerů, 388 uživatelů a 86 respondentů zastává jinou pozici.

Následující otázky měly za úkol zjistit absolutní i relativní čísla týkající se objemu zpráv a podílu spamu. Celkový počet spravovaných schránek v průzkumu dosáhl hodnoty 404687. Mezi jednotlivé pozice byly počty a průměry schránek na respondenta rozloženy takto:

Tabulka 2 – Objemy a podíly spamu podle segmentů

	Součet	*Průměr*	*Medián*	*Směrodatná odchylka*
Postmaster	388057	504	100	39613
IT manager	13394	123	15	454
Manager	491	15	40	139
Uživatel	1353	1,49	3	2,46
Jiná pozice	1392	16	20	1070

Asi největší vypovídací hodnotu má z těchto statistik medián, neboť hodnoty u každé pozice obsahují poměrně značné extrémy, což potvrzují vysoké hodnoty směrodatných odchylek (například po odstranění řádku s nejvyšším počtem schránek u pozice postmaster by došlo ke snížení průměru na 494 a zejména směrodatné odchylky na 1861). Vzhledem k rozdílnosti charakteristik jednotlivých skupin a také k množství respondentů tedy lze za nejpřesnější

statistiku považovat počet e-mailových schránek běžného uživatele, který se asi skutečně bude pohybovat někde kolem dvou nebo tří.

Celkový denní počet zpráv všech respondentů je 398696, což odpovídá celkovému průměru 0,99 zprávy na schránku a den. Tento počet se zdá být poměrně nízký, je však ovlivněn zejména tím, že postmasteři spravují velké množství schránek, které však uživatelé příliš nepoužívají. Naopak lze očekávat, že na tento dotazník odpovídali ne úplně běžní uživatelé, ale spíše uživatelé, kteří mají o problematiku elektronické pošty zájem a jejích služeb využívají relativně častěji. Tuto teorii podporují i průměry rozdělené podle počtu schránek – průměr zpráv na schránku pro respondenty, kteří uvedli nejvíce deset schránek, byl 13,17, ale pro respondenty s více než 10 schránkami byl průměr pouhých 0,92. Potvrzením může být i rozložení mezi jednotlivé segmenty – postmaster 0,70, IT manager 7,12, manager 7,44, uživatel 10,24 a jiná pozice 10,82.

Jednou z nejdůležitějších statistik, která měla z tohoto průzkumu vyplynout je podíl spamu na celkovém množství zpráv. Ihned od počátku průzkumu se podíl ustálil velice blízko třiceti procentům, nakonec se zastavil na čísle 29,4517 % (směrodatná odchylka 24,3588). I rozdíly mezi jednotlivými segmenty jsou poměrně malé: postmaster 23,51 %, IT manager 26,88 %, manager 26,97 %, uživatel 31,88 % a jiná pozice 28,02 % (nižší číslo u postmasterů lze opět zdůvodnit značným množstvím neaktivních uživatelů). Zajímavý pohled přináší přepočet na absolutní čísla resp. denní průměry v tabulce 3.

Tabulka 3 – Podíl spamu a průměrný počet spamu za den

	Podíl spamu	Průměrný počet spamu za den
Postmaster	23,51 %	0,16
IT manager	26,88 %	1,91
Manager	26,97 %	2,01
Uživatel	31,88 %	3,26
Jiná pozice	28,02 %	3,03
Celkem průměr	29,45 %	0,29
Celkem absolutně	29,45 %	117422,75

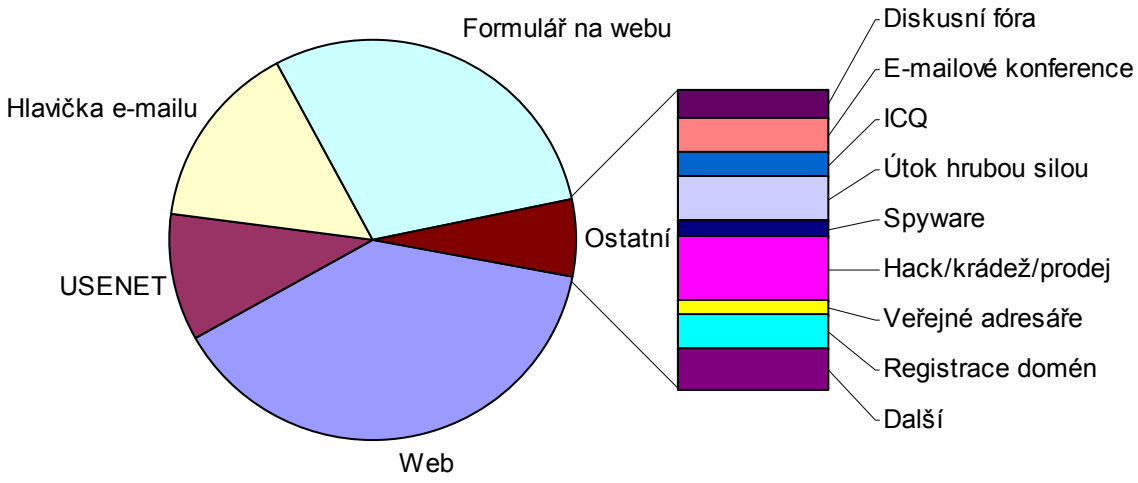
I při celkovém průměru 0,29 spamové zprávy za den to pro průměrného uživatele znamená 106 zpráv ročně. Zajímavý by proto mohl být tento odhad – při jedné a půl schránce na jednoho českého uživatele internetu to znamená zhruba jeden spam na dva uživatele denně. Při počtu uživatelů českého internetu 2,75 miliónu [39] to znamená zhruba 291 miliard zpráv ročně. Podle [40] je průměrná velikost spamové zprávy asi 4,2 kB, což ročně znamená zbytečný přenos asi 1,14 TB dat.

I u podílu spamu je zajímavé porovnání průměrných podílů pro různé počty schránek na uživatele. Pro uživatele, kteří spravují méně než deset schránek tvoří podíl spamu 30,99 %, od deseti do padesáti schránek je to 26 % a pro vyšší počet schránek pouhých 22,09 %. I tento jev lze pravděpodobně vysvětlit přítomností neaktivních uživatelů.

Otázka „Jste si vědom, odkud získal spammer vaši e-mailovou adresu?“ nabízela respondentům možnost vybrat více možností a také doplnit další způsoby. Výsledky by měly být podkladem pro návrh prevence proti spamu.

Obrázek 4 ukazuje poměry jednotlivých způsobů získání e-mailové adresy. Koláčový graf obsahuje přednastavené možnosti, ve sloupcovém grafu jsou uvedeny další způsoby, které uživatelé uvedli slovně. Jako nejčastější způsoby úniku dat byly uváděny ty, které nějakým způsobem souvisí s webem – více než polovina respondentů (385, 56 %) uvedla jako zdroj zveřejnění na webových stránkách, poměrně značný počet se také vyjádřil ve prospěch formulářů na webu (296, 43 %). Ze způsobů, které uživatelé uváděli slovně, byla nejčastěji

zmiňováno nelegální jednání (napadení serveru, krádež dat nebo jejich nelegální prodej, v grafu označeno jako „Hack/krádež/prodej“), skoro v polovině případů spojováno přímo s poskytovateli freemailových služeb (českých i zahraničních). Překvapivě častým zdrojem byl také útok hrubou silou (náhodné generování řetězců, které by mohly tvořit část e-mailové adresy před zavináčem).



Obrázek 4 – Způsoby získání e-mailové adresy

Na otázku „Bráníte se aktivně proti spamu?“ se bohužel vzhledem k chybě ve skriptu ukládajícím hodnoty do databáze nepodařilo získat relevantní odpovědi.

Poslední otázka tohoto bloku zkoumala postoj respondentů ke spamu – „Považujete spam za vážný problém?“ Stejně jako u dalších otázek, které uzavírají jednotlivé bloky, i zde měli dotazovaní možnost vybírat jednu z možností na škále od jedné do pěti (resp. vybírat slovně – rozhodně ano, spíše ano, nevím, spíše ne, rozhodně ne). Průměrné hodnocení této otázky bylo 1,62 (spíše ano, směrodatná odchylka 0,88; četnosti jednotlivých odpovědí [382,240,16,49,3]). Poměrně zajímavý pohled přineslo průměrné hodnocení jednotlivých segmentů – postmaster 1,53, IT manager 1,67, manager 1,91, uživatel 1,63 a jiné pozice 1,45. Postoje postmasterů a běžných uživatelů se daly odhadovat, zajímavá je přece jen vyšší tolerance zejména managerů a IT managerů, u kterých se dal kromě pohledu přímých nákladů také očekávat pohled prizmatem produktivity. Zajímavý je také velice kritický pohled respondentů z jiných pozic.

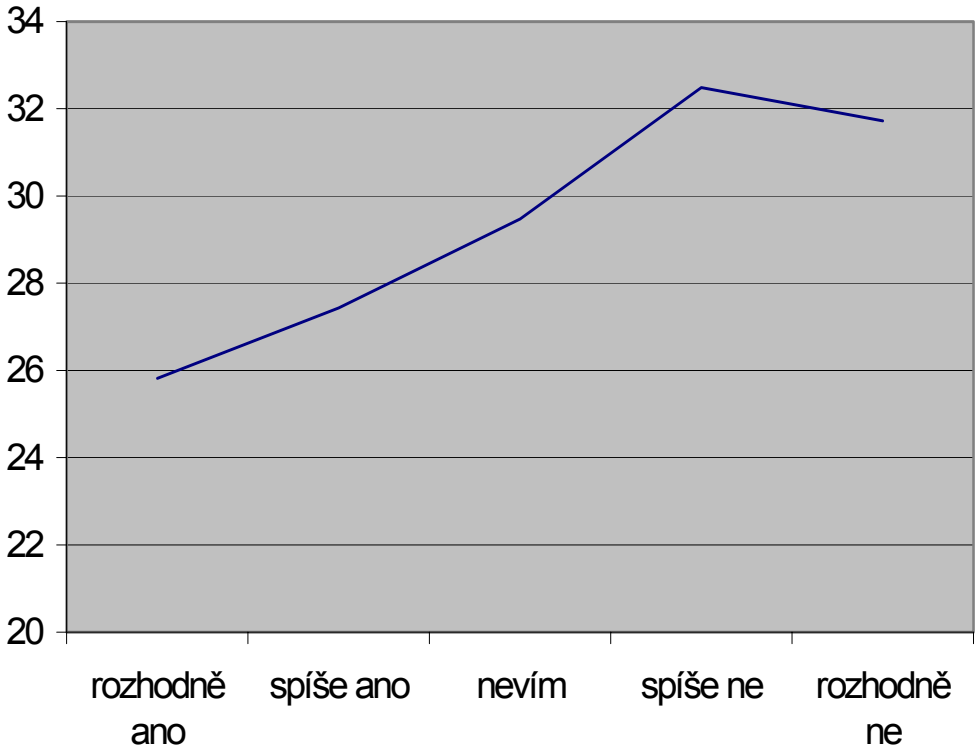
4.3.2.2. Prevence

Cílem bloku nazvaného *prevence* bylo získat informace o tom, zda uživatelé využívají některá z preventivních opatření a jak hodnotí jejich účinnost.

Příjemným překvapením byly určitě výsledky první otázky – „Máte k dispozici rady, jak se spamu vyhnout a jak s ním zacházet?“ 431 respondentů (62 %) uvedlo, že má k dispozici rady, jak se spamu vyhnout. Paradoxně však tito respondenti vykazovali vyšší podíl spamových zpráv než ti, kteří rady k dispozici neměli, rozdíl však byl na hranici významnosti a dal by se vysvětlit například tím, že poučení uživatelé jsou na internetu aktivnější. Rady, jak se spamem zacházet, má k dispozici 411 (59 %) respondentů. Alternativní e-mail pro zveřejnění kontaktních informací nebo jiné riskantní využití používá 552 uživatelů (tedy celých 80 %), 133 nikoliv.

Důležitost prevence v boji proti spamu je průměrně hodnocena známkou 2,83 (nevím; směrodatná odchylka 1,16, četnosti jednotlivých odpovědí [67,269,76,245,29]). Mezi jednotlivými segmenty nebyly zpozorovány výraznější rozdíly – postmaster 2,87, IT manager 2,79, manager 2,85, uživatel 2,84 a jiné pozice 2,73.

Poměrně zřejmá (korelační koeficient 0,95) se ukázala závislost mezi účinností prevence a podílem přijímaného spamu. Respondenti, kteří si myslí, že prevence je dostatečně účinným



Obrázek 5 – Závislost mezi názorem na účinnost prevence a podílem přijímaného spamu

nástrojem, vykazují až o šest procent nižší podíl spamu než ti, kteří prevenci nevěří (viz obrázek 5). Zda je tato závislost vyvolána tím, že důraz na prevenci snižuje podíl spamu nebo naopak tím, že nízký podíl spamu budí dojem, že prevence je účinná, však nelze rozhodnout.

4.3.2.3. Blokování

Blok nazvaný *blokování* měl zjistit přístup respondentů k eliminaci podezřelých zpráv podle různých kritérií. Blokování jako aktivní opatření již zdaleka není tak široce rozšířenou záležitostí jako prevence.

Blokování podle klíčových slov („Filtrujete e-maily podle klíčových slov?“) využívá pouhých 269 (39 %) respondentů, 419 nikoliv. Whitelist, seznam uživatelů, jejichž zprávy jsou bez problému přijaty, je poměrně extrémní metoda, využívá ji („Blokujete poštu od jiných než povolených uživatelů?“) pouze 46 (6,7 %) respondentů, 632 ji nevyužívá. Relativně rozšířené je naopak využívání blacklistů, seznamů zakázaných uživatelů („Blokujete poštu od konkrétních

uživatelů/z konkrétních serverů?“). Vlastní blacklist si vytváří 346 (50 %) respondentů, některý z veřejných používá 39 (5,6 %) dotazovaných. Jako nejčastěji využívané veřejné blacklisty byly uváděny zejména tyto: Open Relay DataBase (ORDB), Mail Abuse Prevention System (MAPS), SpamCop a BrightMail (většinou zprostředkovaně, například na Yahoo!Mail nebo Hotmail). Uživatelé také často využívají služeb více blacklistů zároveň. Blacklisty nepoužívá 316 (46 %) respondentů.

Respondenti byli k blokování jako nástroji na obranu proti spamu poměrně skeptičtí – na otázku „Považujete blokování spamu za účinný prostředek?“ ohodnotili účinnost známkou 3,07 (nevím; směrodatná odchylka 1,12, četnosti jednotlivých odpovědí [31,228,104,279,42]).

Výraznější víru v účinnost blokování projevili ti, kteří se jím zabývají, tedy postmasteři (postmaster 2,64, IT manager 3,01, manager 3,09, uživatel 3,15, jiné pozice 3,15). Minimální rozdíl byl však mezi těmi, kteří některý ze způsobů blokování používají (2,98) a těmi, kteří příchozí poštu vůbec neblokují (3,09).

4.3.2.4. Software

Účinnost a využívání specializovaného software na obranu proti spamu sledoval blok nazvaný *software*. Ani software není příliš často využívaným prostředkem pro obranu proti spamu, neboť 465 respondentů uvedlo, že žádný software nepoužívá.

Nejčastějším modelem nasazení software je nasazení na straně serveru (142 respondentů). Na straně klienta používá software 83 respondentů, online služby využívá 28 dotazovaných. Jako nejčastěji využívané aplikace byly uživateli uvedeny Spam Assassin (69 respondentů) a Spam Killer (24), poměrně značné množství respondentů uvedlo, že využívají vlastní software (11). Častěji byly zmiňovány také samoučící filtr klienta Mozilla, Procmail, Postfix, CloudMark SpamNet, Kerio Mail Server a další – tedy často nikoliv specializovaný software na obranu proti spamu, ale spíše mailové servery nebo klienty s vestavěnými antispamovými funkcemi.

Ačkoliv je úspěšnost software („Považujete software za dostatečně účinný prostředek?“) respondenty z porovnávaných prostředků obrany hodnocena nejvýše, není nijak zvlášť vysoká – průměrné hodnocení je 2,73 (nevím; směrodatná odchylka 1,32, četnosti jednotlivých odpovědí [27,166,215,174,39]). Nejvyšší důvěru v software vkládají postmasteři a manageři (postmaster 2,40, IT manager 2,90, manager 2,52, uživatel 2,77, jiná pozice 2,73). Větší důvěru v software také vkládají ti, kteří některou z podob používají (2,59), zatímco ti, kteří software nepoužívají, hodnotí jeho účinnost na pouhých 2,87.

4.3.2.5. Přímý kontakt

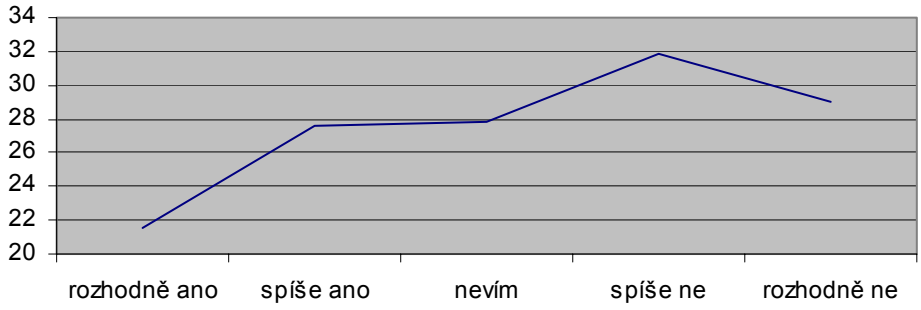
V bloku nazvaném *přímý kontakt* odpovídali respondenti na otázky týkající se stížností přímo u spammera nebo u jeho poskytovatele připojení k internetu (ISP) nebo správce poštovního serveru. Zkoumána byla aktivita, úspěšnost a vnímaná úspěšnost tohoto počínání.

Přímo spammera se pokoušela kontaktovat („Snažil jste se někdy kontaktovat spammera?“) o něco více než polovina respondentů (345, 50 %), z toho 109 (32 %) úspěšně a 236 neúspěšně. Kontaktovat spammera se nikdy nepokoušelo 340 respondentů. Na ISP spammera se obracelo („Snažil jste se někdy kontaktovat poskytovatele připojení/správce pošty serveru, odkud vám přišel spam?“) menší množství respondentů – 199 (29 %), z toho 91 (45 %) úspěšně, 108 neúspěšně. Nikdy ISP spammera nekontaktovalo 488 dotazovaných.

Účinnost přímého kontaktu zúčastněných stran („Myslíte si, že má smysl kontaktovat spammera/jeho ISP?“) hodnotí dotazovaní průměrnou známkou 3,35 (nevím; směrodatná odchylka 1,24, četnosti jednotlivých odpovědí [53,119,99,312,97]). Z jednotlivých skupin jsou nejoptimističtější IT manageři a postmasteři, naopak znatelný pesimismus panuje zejména mezi uživateli – postmaster 3,09, IT manager 3,04, manager 3,27, uživatel 3,52, jiná pozice 3,23.

Rozdíly jsou zřetelné také při rozdělení podle aktivity a úspěšnosti. Respondenti, kteří byli alespoň v jednom případě úspěšní, ohodnotili účinnost kontaktu průměrnou známkou 2,38, neúspěšní naopak pouze 3,34; ti, kteří se o kontakt nepokoušeli vůbec jsou ještě pesimističtější – 3,56.

Mezi postojem k účinnosti přímého kontaktu a podílem přijímaného spamu byla vypozorována poměrně silná závislost (korelační koeficient 0,80). Podíl spamu u respondentů, kteří věří přímému kontaktu byl nižší o šest a více procent než u těch, kteří nepovažují kontakt za účinnou metodu. (viz obrázek 6).



Obrázek 6 – Vztah mezi vnímanou účinností přímého kontaktu a podílem přijímaného spamu

4.3.2.6. Právo

Poslední blok nazvaný *právo* měl za úkol zkoumat možnosti obrany proti spammingu právní cestou. Zkušenosti respondentů s obranou právní cestou jsou minimální – pouze 25 (3,6%) respondentů má z právní obranou zkušenosti („Snažil jste se někdy bojovat proti spammerovi právní cestou?“), z toho 11 (44 %) bylo úspěšných a 14 neúspěšných. O právní obranu se nikdy nepokusilo 662 respondentů.

Právo je také hodnoceno jako nejméně účinný způsob boje proti spamu („Myslíte si, že je současné právo dostatečně účinné v boji proti spamu?“). Průměrná známka je 3,85 (spíše ne; směrodatná odchylka 1,03, četnosti jednotlivých odpovědí [11,41,167,258,209]). Důvěra v účinnost je mezi jednotlivé segmenty rozložena rovnoměrně – postmaster 3,81, IT manager 3,75, manager 3,88, uživatel 3,90 a jiná pozice 3,80. Vzhledem k malému počtu kladných odpovědí má průměrné hodnocení skupin podle aktivity a úspěšnosti poměrně nízkou vypovídací schopnost, rozdíly jsou však velké – úspěšní hodnotili účinnost známkou 2,73, neúspěšní 3,86 a ti, kteří se o právní obranu nikdy nepokoušeli, známkou 3,90. Mezi podílem přijímaného spamu a vnímanou účinností právní obrany nebyla zpozorována závislost (zejména vzhledem k malému podílu respondentů se zkušenostmi s právními protiakcemi).

4.3.2.7. Shrnutí

- Průměrný uživatel spravuje zhruba dvě nebo tři schránky, do každé z nich denně přijme zhruba jednu zprávu. Variabilita těchto hodnot je však velmi vysoká.
- Necelou třetinu zpráv tvoří spamy.
- Pro spammery je nejdůležitějším zdrojem adres web, zejména sbírání zveřejněných adres na webových stránkách a získávání adres pomocí formulářů.
- Respondenti poměrně jednoznačně považují spam za vážný problém.
- Zhruba dvě třetiny respondentů jsou preventivně poučeny o možnostech vyhýbání a zacházení se spamem. Přesto je postoj k účinnosti prevence jako metody obrany proti spamu pouze neutrální.

- Dotazovaní blokují zprávy zejména podle konkrétních uživatelů, kteří jim spamy zasílají, a podle klíčových slov. Žádný z těchto způsobů však nevyužívá více než polovina. Účinnost této metody je hodnocena neutrálně.
- Specializovaný software pro obranu proti spamu používá pouze třetina respondentů, nejčastěji na serveru. Software je považován za nejúčinnější metodu, přesto je jeho účinnost hodnocena jen mírně pozitivně.
- Zhruba polovina dotazovaných se někdy pokusila kontaktovat spammera, zhruba jedna třetina z nich byla úspěšná. Na ISP spammera se obracely necelá třetina, úspěšná však byla skoro polovina z nich. Kontakt je hodnocen mírně negativně.
- Zkušenosti s obranou pomocí právního systému jsou minimální. Respondenti považují účinnost právních protiopatření za nízkou.
- Přestože se dotazovaní cítí být spamem velmi obtěžováni, žádná z metod obrany si nezískala větší důvěru.

4.4. Uvedení problému spamu do kontextu informační bezpečnosti

Britská norma (standard de facto BS 7799, citováno v [37]) definuje informační bezpečnost takto:

Informační bezpečnost je charakterizována jako zachování:

a) důvěrnosti (confidentiality): zajištění stavu, kdy jsou informace přístupné pouze těm osobám, které k tomu mají oprávnění (jsou k tomu autorizovány);

b) integrity (integrity): zajištění takového stavu systému, kdy jsou informace, v něm obsažené, přesné a neporušené;

c) dostupnosti (availability): zajištění stavu, ve kterém mají autorizované osoby přístup k informacím a souvisejícím aktivům v době, kdy to potřebují.

Definice podle standardu de iure ISO/IEC TR 133335-1:1996 přidává také zájem na zajištění zodpovědnosti subjektů a účtovatelnosti akcí, pravosti a spolehlivosti.

Spam se tedy z pohledu těchto definic dotýká zejména *dostupnosti* – nevyžádaná pošta omezuje dostupnost informací, v době, kdy to uživatelé potřebují. Důsledků, které má spam na dostupnost je několik. Spam snižuje dostupnost tím, že zahlcuje poštovní servery a přenosové linky zbytečnými daty a tak způsobuje v lepším případě pouze zpoždění (delay) doručování a přístupu k poště, v horších případech může dojít až k úplnému odmítnutí služby (denial of service, DoS). S problematikou dostupnosti souvisí také další kapacitní problémy, jako je například zabrané místo na disku. Dostupnost je omezena také na straně uživatele – pokud je jeho e-mailová schránka zahlcena spamy, je pro něj složitější se ve zprávách snadno a rychle orientovat.

Důvěrnosti a *integrity* se spam také může dotýkat, ale již v menší míře a spíše zprostředkovaně. Není výjimkou, když spam obsahuje (nebo propaguje) například spyware (software, který sbírá a odesílá citlivé informace z počítače), viry, červy, dialery a podobně, které mohou například zničit citlivá data nebo k nim umožnit přístup.

Informační bezpečnost používá k analýze bezpečnosti tzv. model ohrožení. Ten sestává z těchto prvků:

- aktiva,
- hrozby,

- zranitelnosti,
- dopady,
- protiopatření.

V případě ohrožení spamem představuje *aktiva* firmy (tedy to, co je potřeba chránit) zejména dostupnost elektronické pošty, produktivita zaměstnanců, výše provozních nákladů, data a podobně; je tedy třeba chránit proti zbytečnému zvýšení nákladů způsobeným nevyžádanou elektronickou poštou.

Za *hrozbu* můžeme považovat samotný spam. Ten můžeme považovat za hrozbu lidskou, protože spammer je člověk nebo instituce, a ve většině případů také hrozbu úmyslnou (vědomým záměrem spammera je rozesílat nevyžádanou poštu) a externí (spammer se nachází mimo ohrožený subjekt). Určité hrozby je však možné považovat za interní – například zklamaný zaměstnanec se může firmě mstít tím, že odprodá databázi adres nebo svou nedbalostí způsobí únik těchto dat, čímž způsobí ohrožení subjektu, jehož kontaktní informace neměl dříve spammer k dispozici. Také nevyžádaná pošta rozesílaná hromadně interním subjektem v dobré víře (například hoaxy, řetězové dopisy) může být hrozbou. Poslední uvedené příklady také demonstrují, že ne vždy musí být spam hrozbou úmyslnou. V každém případě je však největším problémem spam externí a úmyslný.

Zranitelnostmi se v informační bezpečnosti myslí nedostatky, slabá místa v bezpečnostním systému nebo jeho části, která mohou být využita hrozbami k útoku na aktiva. V kontextu spamu lze tedy za zranitelnost považovat v první řadě poštovní server (zejména pokud není ochráněn proti spamu), jednotlivě pak všechny e-mailové adresy, jejich adresáře a podobně.

Za *dopady* považuje teorie zejména ztrátu důvěrnosti, integrity a dostupnosti, dále pak ztrátu dobrého jména, know-how, finanční ztráty a fyzická poškození. Konkrétními dopady tedy mohou být například ztráta nebo omezení dostupnosti, vyzrazení dat (e-mailových adres, případně i dalších citlivých údajů), ekonomické ztráty, v extrémním případě i ztráta dobrého jména (pokud bude spammer rozesílat zprávy pod cizími adresami).

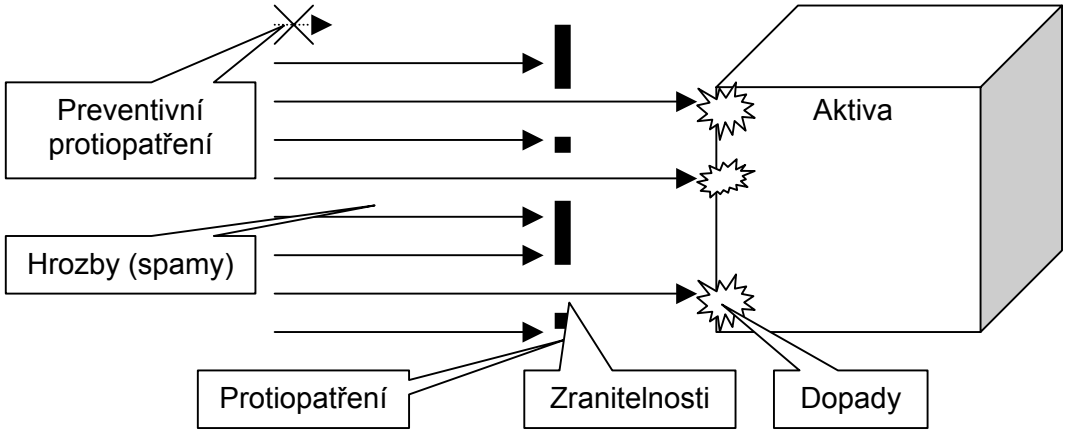
Poslední součástí modelu ohrožení jsou *protiopatření*, jakákoliv zařízení, organizační nařízení, jednání, která snižují zranitelnost systému. Z hlediska působnosti se protiopatření rozdělují na:

- preventivní – působí neustále a snaží se zabránit bezpečnostnímu incidentu,
- dynamická – jsou spouštěna bezpečnostním incidentem,
- reaktivní – jsou aktivována až po bezpečnostním incidentu a slouží k nápravě škod incidentem způsobeným a k tomu, aby se incident znovu neopakoval.

Preventivní protiopatření bývají většinou nejméně finančně náročná (a tedy nejvíce efektivní), naopak nejnáročnější jsou protiopatření reaktivní.

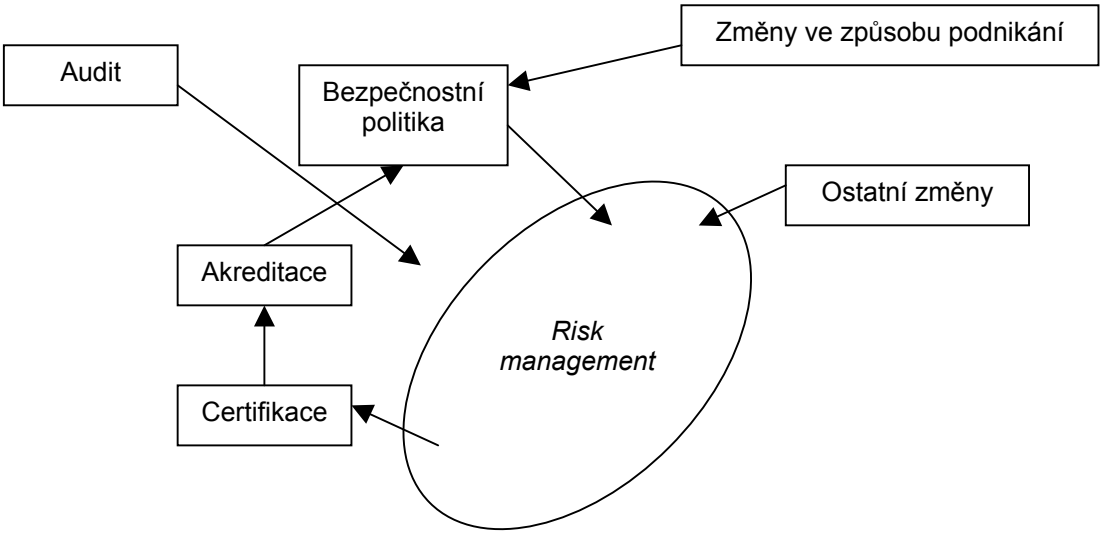
Pro případ spamu byla možná protiopatření analyzována v kapitole *3. Analýza dostupných možností obrany*, do kontextu informační bezpečnosti budou zařazeny později.

Samotný *model ohrožení* pro spam pak vypadá asi takto (obrázek 7):



Obrázek 7 – Model ohrožení spamem

Proces udržování bezpečnosti je možné rozdělit na několik podčástí – přímo udržování bezpečnosti se týká risk management, mimo risk management se nachází zejména bezpečnostní politika, audit a další faktory ovlivňující bezpečnostní politiku a přímo také risk management. Proces udržování bezpečnosti lze zobrazit pomocí tohoto schématu (obrázek 8):



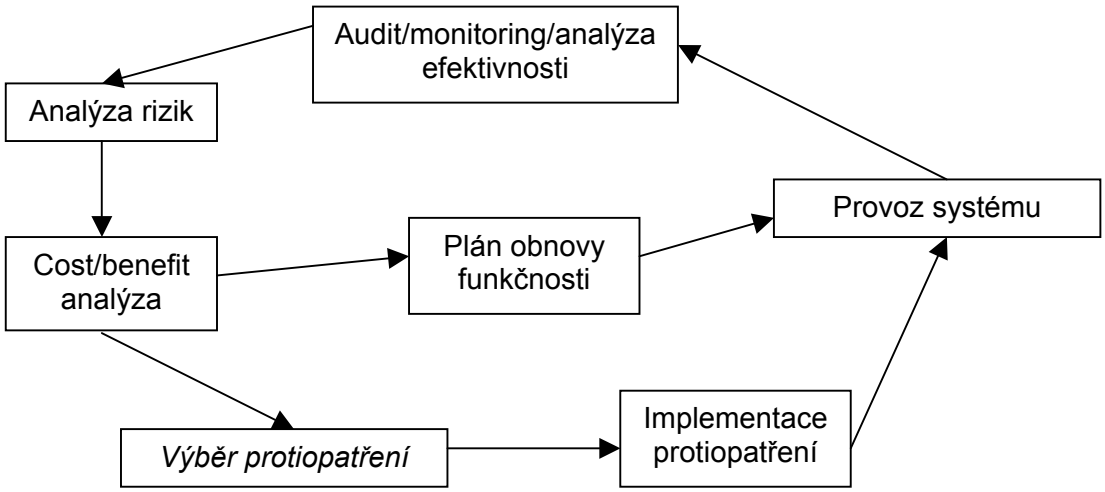
Obrázek 8 – Proces udržování bezpečnosti

V dalším průběhu práce se budu zabývat pouze *risk managementem*, resp. jeho konkrétní částí – *výběrem protiopatření*.

4.5. Risk management

Risk management je klíčovou součástí procesu udržování rizik. Vzhledem k tomu, že risk management je komplexní proces, bude v této kapitole popsán pouze stručně, následující kapitola však bude zaměřena na jednu z jeho částí – výběr protiopatření.

Existuje několik modelů risk managementu, pro tuto práci jsem zkombinoval modely uvedené v [37] a v [38] a doplnil je do formy tohoto grafu:



Obrázek 9 – Model risk managementu

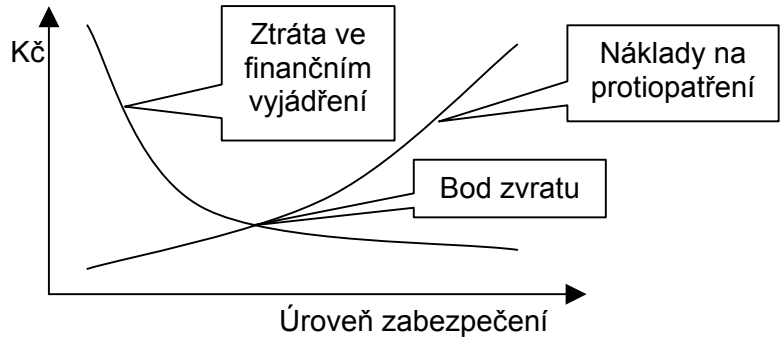
Výchozím bodem v modelu je *analýza rizik*. Cílem analýzy rizik je poskytnout pokud možno objektivní informace o rizicích, a umožnit tak cenově a funkčně optimalizovanou implementaci odpovídajících bezpečnostních protiopatření, která tato rizika snižují na akceptovatelnou úroveň [37]. V případě, kdy rizikem je nevyžádaná pošta, mohou být součástí analýzy rizik (resp. jejích jednotlivých částí) například tyto činnosti:

- analýza hrozeb:
  - analýza objemu příchozího spamu (absolutní hodnoty, průměry, poměrné ukazatele, trendy, odhady),
  - analýza typu spamu (domácí, zahraniční, od velkých spammerů);
- analýza aktiv:
  - analýza/odhady nákladů způsobené spamem (přímé/nepřímé náklady);
- analýza současných protiopatření:
  - analýza účinnosti současných protiopatření,
  - náklady na současná protiopatření;
- analýza zranitelných míst,
- analýza možných protiopatření:
  - analýza nákladů na protiopatření (pořízení, provoz, správa),
  - analýza účinnosti protiopatření;
- analýza možností implementace:
  - analýza možností zařazení správy protiopatření do kontextu řízení IT,
  - časové možnosti a plány.

Výsledkem by měly být podkladové informace pro další fáze správy rizik, typicky ve formě jedné nebo více zpráv.

Na základě výsledků z fáze analýzy rizik je možné provést *cost/benefit analýzu* – analýzu přínosů a nákladů. Vzhledem k tomu, že dosažení vyšší úrovně zabezpečení (a tedy nižších dopadů rizika) je nutné investovat do protiopatření stále vyšší částky, je primárním cílem

analýzy alespoň částečný odhad optimálního nasazení protiopatření. Princip lze ilustrovat grafem (obrázek 10):



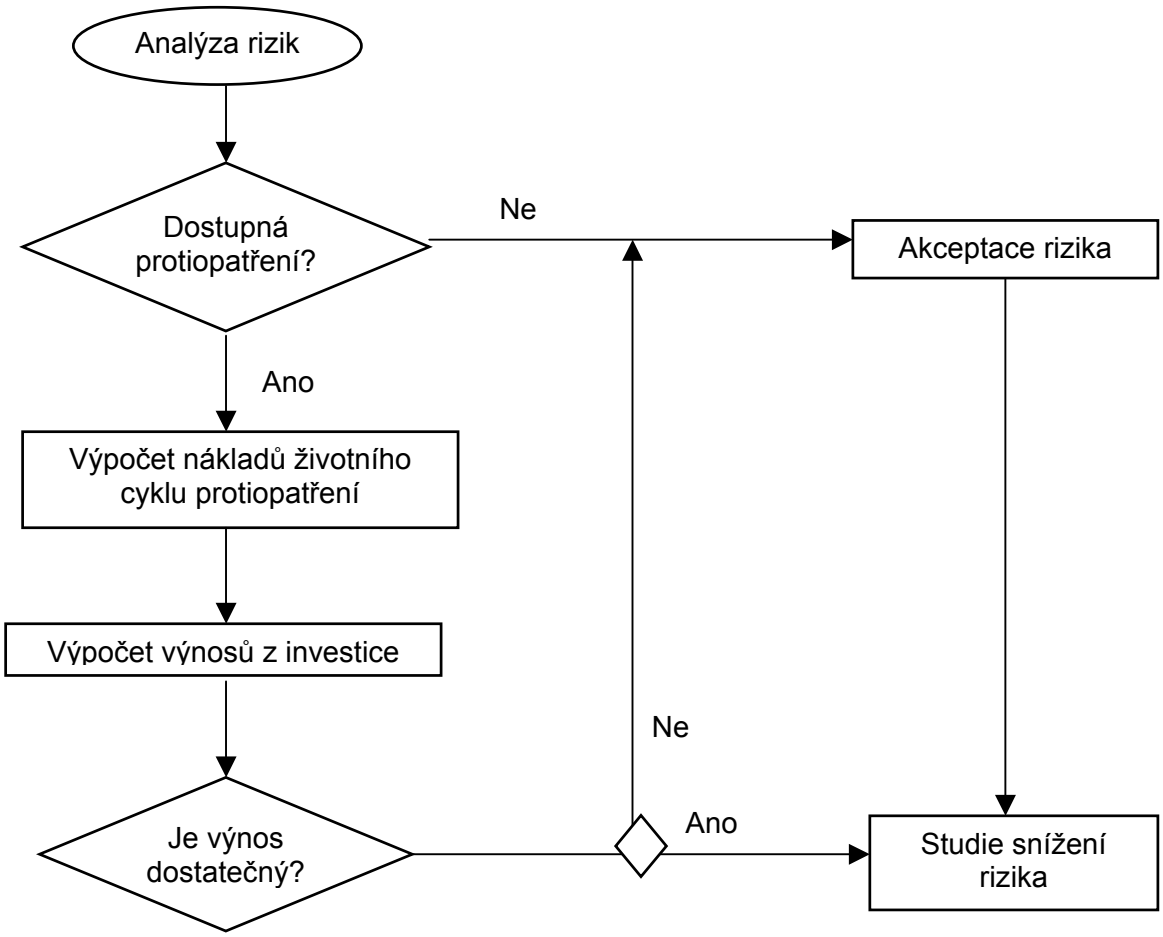
Obrázek 10 – Princip cost/benefit analýzy

Optimální je tedy situace (v obrázku 10 označena jaké „bod zvratu“) při které se vyrovnávají náklady na protiopatření se ztrátou způsobenou rizikem ve finančním vyjádření. Graf je však pouze zjednodušením situace, prakticky je vhodnější využívat tuto rovnici:

$$(-\Delta \text{ ztrát}) - \text{náklady na protiopatření} \geq 0$$

kterou lze interpretovat takto: snížení ztrát ve finančním vyjádření by mělo převyšovat náklady na protiopatření. V případě, že tato situace nemůže nastat (náklady na opatření by ve všech situacích převyšovaly ztráty nebo protiopatření nejsou vůbec dostupná), je nutné riziko akceptovat a snažit se jej alespoň snížit.

Proces cost/benefit analýzy lze ilustrovat následujícím vývojovým diagramem (obrázek 11, převzato z [38]):



Obrázek 11 – Proces cost/benefit analýzy

Výstupem C/B analýzy by tedy měla být zpráva (studie snížení rizika), která obsahuje rozhodnutí o nasazení protiopatření a podklady pro jeho výběr z pohledu nákladů, nebo naopak rozhodnutí o akceptaci rizika a případném snížení rizik.

Poznámka: často se C/B analýza uvádí v procesu risk managementu až za fází výběru protiopatření. Ve skutečnosti však tato analýza prostupuje celým procesem – před výběrem protiopatření jako získání vstupních dat pro výběr (nebo případné zrušení výběru), během výběru protiopatření jako analýza efektivnosti *konkrétních* protiopatření i během provozu systému (resp. monitoringu).

Další fází, *výběrem protiopatření* se bude podrobně zabývat následující kapitola.

V případě, že není možné vybrat nákladově vyhovující protiopatření, je nutné riziko akceptovat a na základě studie snížení rizika vytvořit *plán obnovy funkčnosti* – připravený plán, činností, které budou prováděny při výskytu rizika (v tomto případě dramatickém zvýšení objemu příchozího spamu). V kontextu spamu může tento plán představovat například rychlé, ale krátkodobé zavedení některého ze způsobů filtrování (blacklist, whitelist) a zrychlený proces zavedení dalších protiopatření.

Poté, co jsou vybrána vyhovující protiopatření, je nutné je *implementovat* – uvést do provozu. V této fázi je tedy proveden nákup nebo vývoj odpovídajícího software, jsou vytvořena a zavedena organizační opatření, prováděno testování, customizace, přizpůsobeny procesy, organizační struktura a podobně. Výsledkem by mělo být předání funkčního systému do běžného provozu.

Provoz systému představuje běžný chod systému s poměrně malým rozsahem zásahů ze strany člověka. Nedílnou součástí provozu je také *audit/monitoring/analýza efektivnosti* – funkčnost systému se porovnává podle tvrdých i měkkých metrik, jejich výsledky pak slouží jako vstup pro další analýzu rizik, cost/benefit analýzu a podobně. Jako vhodné metriky lze například využít podíl příchozího spamu, podíl spamu, který projde přes protiopatření, podíl false positives, hardwarová náročnost protiopatření, lidská náročnost protiopatření, finanční náročnost, finanční ztráty způsobené spamem a podobně.

Lze tedy říci, že risk management je v důsledku vývoje na straně rizika i na straně opatření kontinuální a neustále se opakující proces.

4.6. Výběr protiopatření – metodický postup

Vstupem do procesu výběru protiopatření by měly být data z analýzy rizik, zejména tedy analýza hrozeb, zranitelností a analýza současných a možných protiopatření, a dále možnosti dané cost/benefit analýzou, která určuje, zda bude riziko akceptováno nebo zda se půjde cestou protiopatření. V případě volby protiopatření je nutné vybrat účinností i náklady vyhovující protiopatření v těchto třech fázích procesu výběru:

1. Analýza konkrétních možností protiopatření.
2. Specifikace kritérií výběru/řešení
3. Výběrové řízení.

Výstupem by měly být zvolená protiopatření a pokyny pro jejich implementaci.

4.6.1. Analýza konkrétních možností protiopatření

Vstupy	• analýza rizik (analýza hrozeb, zranitelných míst, protiopatření, aktiv…) • studie snížení rizika (rozhodnutí o nasazení protiopatření, nákladová omezení) • současný stav protiopatření (účinnost, životnost, smlouvy) • externí zdroje
Výstupy	• plán nasazení protiopatření
Zodpovědnosti	• IT manager
Popis činnosti	• vytvoření plánu nasazení protiopatření • volba optimální kombinace jednotlivých typů protiopatření

Jak bylo zmíněno dříve protiopatření lze rozdělit podle času působení na preventivní, dynamická a reaktivní. Podle druhu protiopatření na administrativní, technická a fyzická (i když fyzická se v této problematice neuplatňují). Proto je možné jednotlivé druhy možných protiopatření rozdělit do takovéto tabulky (tabulka 4):

Tabulka 4 – Rozdělení protiopatření

	Administrativní	*Technická*
Preventivní	• politiky zveřejňování adres • politiky používání adres (primární a sekundární, veřejné a soukromé a podobně) • návody pro bezpečné používání elektronické pošty	• maskování adres • formuláře pro odesílání zpráv • používání adres neodhadnutelných slovníkem nebo hrubou silou • jednorázové adresy • ochrana databází s adresami
Dynamická	• návody pro postižené uživatele	• blacklisty • whitelisty • analýza obsahu • analýza hlaviček • komplexní software • antivirová kontrola
Reaktivní	• hlášení spamu správci protiopatření • stížnosti k rukám spammera • stížnosti k rukám ISP • právní akce	• smazání spamu • přizpůsobení protiopatření

Cílem této fáze je zejména vytvořit strukturu nasazení protiopatření – jaká protiopatření budou nasazena v kontextu podle času (preventivní/dynamická/reaktivní). Doporučená protiopatření jsou uvedena v kapitole *Doporučení (Best Current Practices)*.

Klíčem pro výběr protiopatření by měla být analýza zranitelností a dopadů, které z těchto zranitelností hrozí. Podle nich je možné určit prioritu nasazování jednotlivých protiopatření. K dispozici je zde několik strategií postupu, například tyto:

- odstranit všechny zranitelnosti,
- nejprve odstranit ty, které lze odstranit zdarma, dále podle rozpočtu,
- jako první odstranit ty, které mají potenciál způsobit největší ztráty.

Výsledky cost/benefit analýzy by zde měly sloužit spíše jako omezení, v této fázi není možné přesně určit celkové náklady na protiopatření.

Plán by tedy měl obsahovat:

- v kterých oblastech a jaká protiopatření budou nasazena:
  - preventivní,
  - dynamická,
  - reaktivní,
  - technická,
  - administrativní;

- v jakém časovém horizontu bude nasazení provedeno;
- jakým způsobem budou protiopatření realizována:
  - interně (zejména pro administrativní opatření to může být jediná volba),
  - externě nákupem,
  - externě outsourcingem;

Ukázka plánu nasazení protiopatření:

Preventivní opatření – měly by být zavedeny politiky používání a zveřejňování adres, uživatelé by měli být seznámeni s pravidly pro bezpečné používání elektronické pošty. Každý uživatel by měl mít k dispozici e-mailovou adresu pro běžné použití a adresu pro korespondenci s důvěryhodnými subjekty.

Dynamická opatření – zavedení komplexního software by mělo snížit počet spamových zpráv, které dorazí až k uživateli. Zároveň by se měla zavést antivirová kontrola veškeré příchozí pošty k zamezení dalších škod.

Reaktivní opatření – spam, který projde sítem software by měli postižení hlásit, aby se mohlo přizpůsobit nastavení pravidel. V případě větších útoků na poštovní server (útok hrubou silou, slovníkový útok, rozeslání zpráv na velké množství adres) zvažovat možnost právní nebo jiné obrany.

Do jednoho měsíce by měly být připraveny specifikace kritérií výběru. Interně budou realizována preventivní a reaktivní opatření, dynamická opatření budou dodána externím subjektem.

4.6.2. Specifikace kritérií výběru/řešení

Vstupy	• plán nasazení protiopatření
Výstupy	• kritéria výběru • specifikace řešení
Zodpovědnosti	• správa IT (správci poštovních serverů, sítě a podobně)
Popis činnosti	• specifikace konkrétních metod obrany v souladu s efektivností a nákladovými omezeními • specifikace kritérií na protiopatření pro nákup nebo interní řešení

Poté, co je vytvořen plán nasazení protiopatření, je třeba jej upřesnit z technického pohledu – vytvořit kritéria pro výběr nebo implementaci protiopatření.

Kritériem, které má specifickou hodnotu je cena resp. náklady řešení. V procesu zavádění protiopatření stojí naproti rozpočtovým omezením resp. snížení dopadu daným protiopatřením. Srovnání však není úplně jednoduchá záležitost, protože náklady na protiopatření mají mnoho podob:

- Jednorázové náklady – náklady na pořízení software, hardware; náklady na implementaci…
- Periodické náklady – aktualizace, přístupy do databází, periodická údržba…
- Náklady na správu – úprava protiopatření (reakce na vývoj, ladění…), manuální vstupy…

Zatímco zavedení administrativních opatření generuje většinou pouze jednorázové náklady a jejich účinnost může být dlouhodobá, zejména u aktivních technických opatření lze počítat se značnými náklady na jejich provoz (pro zachování minimálně konstantní účinnosti).

Druhým klíčovým kritériem je účinnost – míra, v jaké zvolená protiopatření sníží dopady. Je však třeba počítat nejen s přímým snížením nákladů, ale na druhou stranu také s případným zvýšením nákladů v důsledku zavedení protiopatření – false positives, obtěžování uživatelů a podobně.

Je možné specifikovat velké množství dalších kritérií, v následujícím seznamu jsou však uvedeny pouze některá obecně využitelná pro výběr aktivních opatření (specializovaný sw, filtry a podobně):

- možnosti customizace:
  - správa pravidel – možnost přidávání vlastních pravidel, možnost editace/mazání pravidel stávajících, možnost nastavení vah jednotlivých pravidel;
  - nastavení účinnosti – možnost volit kompromis mezi účinností a false positives, nastavení prahových hodnot;
  - doplnění dodatečných modulů – rozšíření systému o další možnosti (propojení, algoritmy a podobně);
  - tvorba vlastních blacklistů/whitelistů – možnost přidávání/editace odesílatelů (podle serveru/adresy/domény), používané metody autorizace a upozorňování uživatelů;
- dostupnost externích dat:
  - provázání s externími databázemi – možnost propojení na veřejné blacklisty, možnost generického propojení, možnosti replikace;
  - aktualizace pravidel – možnosti periodické aktualizace pravidel, frekvence, cena (tvorba ceny – jednorázová platba, předplatné na období, platby za jednotlivé aktualizace), řešení konfliktů aktualizovaných pravidel s pravidly upravenými uživatelem;
- obsažené know-how:
  - předdefinovaná pravidla – způsob získání pravidel, pravidla kontrolují hlavičku/text/formátování zprávy;
  - aktualizace pravidel – viz výše;
  - obsažené algoritmy – porovnávání, samoučící algoritmy, bayesiánské filtrování, fuzzy logika, porovnávání otisků zpráv, vícekriteriální hodnocení (algoritmy výpočtu);
- usnadnění administrativních opatření:
  - reporting spamu – možnost jednoduše reportovat spam správci, subjektu spravujícímu databázi pravidel/blacklist;
  - automatizovaný kontakt spammera/ISP – možnost analýzy hlaviček k získání kontaktních údajů, předpřipravené stížnosti;
- náročnost na výkon:
  - hardware – náročnost na CPU, paměť, prostor na disku;
  - připojení – stahování celých zpráv, stahování pouze hlaviček, mazání na serveru;

a mnoho dalších.

Ukázka kritérií výběru:

Požadavky na software – spolupráce se serverem Microsoft Exchange 2000, možnost provozu na stávajícím hardware, obsaženy předdefinované pravidla s možností aktualizace přes internet

a editace/doplnění vlastních pravidel, možnost propojení na více externích blacklistů, možnost tvorby vlastního blacklistu.

4.6.3. Výběrové řízení

Vstupy	• kritéria výběru • plán nasazení protiopatření • cost/benefit analýza, rozpočty
Výstupy	• smlouvy • pokyny pro implementaci
Zodpovědnosti	• IT manager
Popis činnosti	• výběr konkrétních protiopatření • jednání o realizaci projektu • uzavření smluv

V případě, kdy se v předchozích krocích rozhodne o externím nákupu nebo outsourcingu řešení, je jednou z možností provedení výběrového řízení. To se v případě výběru protiopatření proti spamu prakticky neliší od jiných výběrových řízení, proto zde nebude detailně popisováno.

4.7. Doporučení (Best Current Practices)

Zde se pokusím shrnout nejčastěji zmiňovaná a tedy snad i nejpoužívanější doporučení, která se týkají zabezpečení proti spamu. Opatření je velké množství, problematika se stále dynamicky vyvíjí, proto nelze tato doporučení brát jako definitivní.

4.7.1. Preventivní protiopatření

Preventivní opatření jsou vhodná nejen pro subjekty, které zatím nemají se spamem problémy, i pro ty, které již spam dostávají. Dobře zvolená preventivní opatření snižují na minimum možnost, že budou adresy zveřejněny a tak se dostanou do rukou spammerům. Podobně zavedení preventivních opatření pro případy, kdy již subjekt spam dostává může být účinně ze dvou důvodů:

1. noví spammeři se již nemusí dostat k adresám,
2. předpokládá se, že trvanlivost adres, které spammeři používají je poměrně krátká, proto může dojít i k snížení objemu přijímaného spamu.

Zjistit fakta o účinnosti protiopatření je poměrně problematická záležitost. Jako určité vodítko k volbě protiopatření mohou sloužit návody a průzkumy zveřejňované v tisku, knihách a zejména na internetu. Jako základní východiska pro implementaci *preventivních opatření* lze považovat tato:

- klíčovým kanálem, přes který získávají spammeři adresy, je web;
- ačkoliv existují i jiné možnosti, ve většině případů jsou spammeři zaměřeni na adresy uvedené v nemaskované podobě, typicky jako odkazy;
- útoky slovníkem nebo hrubou silou nejsou výjimečné.

Preventivní opatření by tedy měla být vedena tímto směrem:

- důsledně používat primární (soukromé) a sekundární (veřejné) adresy;

- při každém zveřejnění důsledně promyslet, zda přínosy zveřejnění vyrovnávají riziko;
- na webu zveřejňovat pouze veřejné adresy a to nejlépe v maskované podobě;
- adresy by měly být dostatečně dlouhé a špatně odhadnutelné (aby odolaly útokům hrubou silou a slovníkovým útokům);
- databáze s adresami by měly být dostatečným způsobem zabezpečeny;
- pro velice rizikové záležitosti používat pouze jednorázové adresy;
- při hromadném rozesílání zpráv zadávat adresáty do pole Bcc, upozorňovat ty, kteří tak nečiní.

Některá z administrativních opatření (používání adres, jejich zveřejňování a podobně) vyžadují součinnost všech zaměstnanců, proto je nutné opatření navrhnout vhodným způsobem (zejména s ohledem na co nejmenší požadavky na zaměstnance) a dostatečně a srozumitelně je osvětlit.

Preventivní opatření také mohou ztěžovat kontakt ostatním subjektům (zejména některé druhy maskování) – při jejich návrhu by se mělo přihlížet k rozumnému kompromisu mezi bezpečností a použitelností.

4.7.2. Dynamická protiopatření

Za těžiště obrany proti spamu lze považovat opatření *dynamická* – ta, která řeší ohrožení ve chvíli, kdy nastane. Pro subjekty, které již spamy dostávají, vedou tato opatření k asi největšímu poklesu ztrát, ale i subjekty, které zatím nejsou spamem ohrožovány, by měly mít nachystané alespoň základní opatření pro případné ohrožení v budoucnu.

Zejména zahraniční spam se v poslední době vyskytuje v obrovském množství a mnoha podobách a často je již vytvářen s tím, aby dokázal používaná protiopatření obejít. Proto je systém protiopatření postavený na jednoduchých pravidlech poměrně neúčinný (v některých případech, jako například filtrování top-level domén nebo whitelisty, může být účinný, ale pouze za cenu omezení samotné e-mailové komunikace nebo velkého množství false positives). Jako nejúčinnější se proto ukazuje nasazení specializovaného software, které kombinuje množství filtrů nebo nabízí sofistikované algoritmy.

V současné době se naštěstí stává samozřejmou antivirová kontrola – není to problém pouze spamu, ale právě u spamu je podíl zavirovaných zpráv poměrně značný. Proto lze jistě doporučit používání antivirových programů, ideálně přímo na poštovním serveru.

Pokud přece jen uživatel spam přijme, měl by být instruován, jak s ním zacházet. Podobně jako u preventivních opatření platí i zde vhodný návrh pravidel a jejich zřejmost. Pravidla by měly obsahovat minimálně varování před otevíráním příloh, klepáním na odkazy nebo žádostmi o vyřazení (alespoň u podezřelých zpráv).

V každém případě je při zavádění dynamických opatření nutné vhodně nastavit prahy tak, aby bylo zachyceno co největší množství spamu při co nejnižším poměru false positives. Vzhledem k tomu, že ztráty způsobené false positives i náklady na manuální kontrolu, zda mezi odfiltrovanými zprávami není některá legitimní, jsou vysoké, je vhodné při nastavení dát přednost co nejnižšímu poměru false positives. Vhodným podkladem pro přesné nastavení může být reportování spamu postiženými uživateli.

Pro dynamická opatření tedy platí tato doporučení:

- vhodné je využití sofistikovaného software (nebo online služeb), kombinujícího více přístupů;
- pro větší počet uživatelů je nejvhodnější nasazení na serveru, nasazení na klientovi je vhodné pouze pro domácí uživatele;

- asi nejúčinnější dostupnou metodou je analýza zpráv;
- účinnost veřejných blacklistů je diskutabilní, riziko false positives je obrovské;
- používání whitelistů pro odesílatele, jejichž zprávy by mohly být označeny jako podezřelé, velmi snižuje hrozbu false positives;
- organizační opatření (zákaz otevírání příloh, klepání na odkazy, žádostí o vyřazení) mohou efektivně snížit dopady příchozího spamu.

4.7.3. Reaktivní protiopatření

Reaktivní protiopatření mají za úkol zamezit ztrátám, které by vznikly při opakování ohrožení v budoucnosti. Asi jedinou možností, která toto zajišťuje je přizpůsobení nastavení protiopatření na základě nezachyceného spamu. Smazáním spamu, který prošel až do schránky, uživatel alespoň uvolní místo na disku. Nahlášením spamu může uživatel přinést cenné údaje pro nastavení systémů obrany do budoucna.

Výsledky dalších možností jsou nejisté. Kontaktování spammera může přinést zastavení operací z jeho strany stejně jako jejich zesílení. Větší šance na úspěch má stížnost u ISP, přes jeho servery byla zpráva odeslána, i zde ale záleží na tom, jaký postoj k celé věci zaujme druhá strana. Právní akce (stížnosti, žaloby) jsou stále poměrně extrémní, jak ale ukázala kauza Tvujdum.cz, nejsou úplně bez šance na úspěch. Situace zde ale souvisí s vymahatelností práva, v každém případě by tato možnost uplatněná zejména na lokální spammery mohla přinášet (alespoň dlouhodobě) pozitivní výsledky.

Doporučení pro reaktivní opatření:

- smazáním evidentního spamu se uvolní místo na disku a sníží riziko nakažení viry;
- hlášení neodfiltrovaného spamu může přinést cenné podklady pro další boj proti spamu;
- v případě většího množství zpráv od jednoho spammera je vhodné kontaktovat jeho ISP;
- právní obrana se vyplatí využít pouze u českých spammerů.

4.8. Závěr kapitoly

V úvodu kapitoly byly shrnuty výsledky několika průzkumů, zejména vlastního dotazníkového šetření, které potvrdilo, že spam je vnímán jako vážný problém. Za nejúčinnější metodu je považováno používání specializovaného software.

Problém spamu je součástí informační bezpečnosti – spam je hrozbou, která ohrožuje zejména dostupnost elektronické pošty, provozní náklady a produktivitu zaměstnanců. Pro řízení rizik je proto vhodné využít existující metodologie udržování bezpečnosti.

Pro úspěšný boj se spamem je nutné nasadit správná protiopatření. Klíčem pro jejich výběr by mělo být porovnání snížení nákladů, které spam přináší, a nákladů na protiopatření. Je vhodné implementovanými protiopatřeními pokrýt všechny fáze napadení – preventivními zamezit napadení, dynamickými eliminovat důsledky napadení a reaktivními snížit ztráty způsobené v budoucnu. Důsledná specifikace kritérií a výběrové řízení mohou dále zefektivnit proces výběru protiopatření.

Existují doporučené postupy a opatření proti spamu, některé z nich jsou uvedeny v poslední části kapitoly. Vzhledem k dynamice problematiky se však nedají považovat za definitivní a je nutné je vždy přizpůsobit situaci.

Závěr

Shrnutí výsledků

V úvodu této práce jsem si stanovil dva cíle – zmapovat problematiku spamu z co nejširšího pohledu a výsledky spolu s vlastním dotazníkovým šetřením využít k aplikaci metodik informační bezpečnosti na oblast spamu se zaměřením na výběr protiopatření.

První kapitola zmapovala základní koncepty problematiky spamu. Spam byl definován a klasifikován podle několika různých hledisek. Byly zde také vyjmenovány významy spamu; význam marketingový (a tedy motivace spammerů) a význam spamu jako problému, který motivuje k zavádění protiopatření. Kapitola také obsahuje historické souvislosti spammingu, jeho stav v současnosti a odhadovaný význam v budoucnosti. V poslední části je spam analyzován z pohledu jednotlivých účastníků a jsou zde také uvedeny základní znaky technického provedení rozesílání spamů.

Druhá kapitola se zabývá rozborem nákladů souvisejících se spamem rozděleným do třech částí – analýza přímých nákladů, nepřímých nákladů a zvlášť uvedena analýza nákladů na boj proti spamu. Náklady jsou analyzovány podle jednotlivých účastníků a potvrzují jednu ze základních myšlenek této práce – náklady spammera jsou ve srovnání s náklady postižených účastníků minimální, náklady postižených jsou však rozdrobeny. Celkové náklady způsobené spamem se pohybují v řádu desítek miliard dolarů.

Cílem třetí kapitoly bylo zmapovat možná opatření proti spamu. Ta byla rozdělena na preventivní, dynamická a reaktivní. U každého druhu protiopatření jsem uvedl většinu nejpoužívanějších a nejúčinnějších metod. Snížit náklady lze zejména využitím preventivních opatření, která spočívají v zamezení zveřejnění adres pro spammery, a opatření dynamická, u kterých se jedná o identifikaci spamu mezi příchozími zprávami a jeho eliminaci. Reaktivní opatření mohou být účinná ve snižování budoucích nákladů, většinou však za cenu vysokých nákladů na opatření samotná a velké pravděpodobnosti neúspěchu.

Poslední kapitola shrnuje dohromady podklady z předchozích kapitol, vlastní dotazníkové šetření, další průzkumy a metodiky informační bezpečnosti k vytvoření postupu a doporučení k minimalizaci nákladů způsobených spamem. Vlastní dotazníkové šetření ukázalo, že uživatelé internetu vnímají spam jako vážný problém a žádnou z metod nepovažují za dostatečně účinnou (za nejúčinnější považují využívání specializovaného software, ani s jeho účinností však není výrazná spokojenost).

Klíčovou součástí je aplikace metodik udržování informační bezpečnosti na problematiku spamu. Kapitola nejdříve shrnuje základy informační bezpečnosti a strukturu procesu udržování bezpečnosti, těžištěm však je výběr protiopatření. Postup výběru protiopatření je detailně popsán, jsou zde také dána doporučení pro výběr protiopatření.

Přínos práce

Asi největším přínosem práce je aplikace problematiky spamu na metodiky informační bezpečnosti. Spam tak není vnímán jen jako problém týkající se pouze elektronické pošty, ale jako hrozbu, která může vést nejen k ekonomickým ztrátám, a tak by měla být brána na dostatečnou váhu. Pro rozhodnutí o zavedení protiopatření práce obsahuje návrh postupu a detailní informace, kritéria a doporučení pro výběr protiopatření.

Přínosem je také poměrně široké zmapování problematiky spamu, zejména nákladová analýza a analýza dostupných protiopatření.

Zajímavé informace o problematice spamu mohou přinést výsledky vlastního dotazníkového šetření, které bylo provedeno na poměrně rozsáhlém vzorku uživatelů.

Seznam použité literatury

[1] MAIL ABUSE PREVENTION SYSTEM. Definition of spam. Citováno 14.2.2003. *http://mail-abuse.org/standard.html*

[2] ANTISPAM.CZ. Spamming: Podstata problému. Citováno 14.2.2003. *http://www.antispam.cz/info/f_prob.htm*

[3] SPAM.COM. Spam in time. Citováno 14.2.2003. *http://www.spam.com/*

[4] WEBOPEDIA. Spam (encyklopedické heslo). 24.1.2003. Citováno 14.2.2003. *http://www.webopedia.com/TERM/s/spam.html*

[5] MONTY PYTHON. Monty Python‘s Flying Circus: Episode 25. TV seriál. BBC, 15.12.1970. Citováno 14.2.2003. Přepis scénáře například na *http://www.detritus.org/spam/skit.html*

[6] BARRET, Daniel J. Bandité na informační dálnici. Praha, Computer Press, 1999. ISBN 80-7226-167-3.

[7] THE 419 COALITION. The Nigerian Scam Defined. Citováno 16.2.2003. *http://home.rica.net/alphae/419coal/*

[8] BBC. MacIntyre – Reportáž točená inkognito: Miliardové podvody. Uvedeno v České televizi, leden 2003.

[9] MAGEE, Mike. Americans to loiter in London hotel lobbies. The Inquirer, 11.12.2002. Citováno 5.3.2003. *http://www.theinquirer.net/?article=6680*

[10] CAUCE. The Problem. Citováno 6.3.2003. *http://www.cauce.org/about/problem.shtml*

[11] HLAVENKA, Jiří. Internetový marketing: praktické rady, tipy, návody a postupy pro využití Internetu v marketingu. Praha, Computer Press, 2001. ISBN 80-7226-498-2.

[12] STUCHLÍK, Petr; PEGNER, Martin; DVOŘÁČEK, Martin. Marketing a reklama na internetu. Praha, Grada, 1998. ISBN 80-7169-630-7.

[13] LYNCH, Keith. Keith Lynch‘s timeline of spam related terms and concepts. 23.11.2002. Citováno 8.3.2003. *http://keithlynch.net/spamline.html*

[14] BRIGHTMAIL INCORPORATED. Brightmail Dominates Anti-Spam Technology Market. Tisková zpráva Brightmail Inc. 30.4.2002. Citováno 10.3.2003. *http://www.brightmail.com/pressreleases/043002_radicati.html*

[15] LIST-NEWS.COM. Spam Load Nearly Doubles in a Year: Jupiter. 19.9.2002. Citováno 10.3.2003. *http://list-news.com/articles/02september/20020919.html*

[16] KOPTA, Martin. Sisyfovský boj proti spamu. Lupa, 15.3.2001. Citováno 10.3.2003. *http://www.lupa.cz/clanek.php3?show=1418*

[17] THE SPAMHAUS PROJECT. SBL Advisory: Rationale. Citováno 2.4.2003. *http://www.spamhaus.org/sbl/sbl-rationale.html*

[18] WENDLAND, Mike. Spam king lives large off others‘ e-mail troubles. The Freep (Detroit Free Press), 22.11.2002. Citováno 2.4.2003.
http://www.freep.com/money/tech/mwend22_20021122.htm

[19] RAZ, Uri. How do spammers harvest email addresses? Citováno 2.4.2003.
http://www.private.org.il/harvest.html

[20] VAKNIN, Sam. The Economics of Spam. Citováno 4.4.2003.
http://samvak.tripod.com/busiweb32.html

[21] WAGNER, Mitch. Reports: Spam Costs $11.9 Billion; Users Favor Legal Ban. InternetWeek.com, 3.1.2003. Citováno 4.4.2003.
http://www.internetwk.com/breakingNews/INW20030103S0006

[22] CHUA, Louis. Electronic bombardment. Computerworld Singapore. Citováno 5.4.2003.
http://computerworld.com.sg/pcwsg.nsf/unidlookup/FB817084FCC5506948256CFB00176BCA?OpenDocument

[23] VOJÍŘ, Aleš. Lidé si mohou stěžovat na nechtěné e-maily. Hospodářské noviny, 31.05.2002, str.4.

[24] PROFIT. Spam způsobuje ve světě ztráty miliard dolarů. Profit Speciál, 3.2.2003, č.6, str.7.

[25] EURO. Miliardy ve vzduchu. Euro, 3.2.2003, č.005, str.32.

[26] METZ, Cade. Personal Antispam Tools. PC Magazine, 25.2.2003. Citováno 8.4.2003.
http://www.pcmag.com/article2/0,4149,849485,00.asp

[27] GRAHAM, Paul. A Plan for Spam. Srpen 2002. Citováno 8.4.2003.
http://www.paulgraham.com/spam.html

[28] GALLAGHER, Sean. Fight Spam With Spam. Baseline, 6.3.2003. Citováno 18.4.2003.
http://www.baselinemag.com/article2/0,3959,920545,00.asp

[29] ZEMAN, Mirek. Tvujdum dostal pokutu za rozesílání spamu. Lupa, 3.4.2003. Citováno 12.4.2003.
http://www.lupa.cz/clanek.php3?show=2779

[30] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Monitorování elektronické pošty a ochrana soukromí a osobních údajů zaměstnanců. Úřad pro ochranu osobních údajů k problémům z praxe – č.1/2003. Citováno 15.4.2003.
http://www.uoou.cz/stan_praxe_1_2003.php3

[31] EVROPSKÁ KOMISE. Communications Data Protection Directive 2002/58/EC. Prosinec 2002. Citováno 15.4.2003.
http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

[32] CENTER FOR DEMOCRACY & TECHNOLOGY. Why Am I Getting All This Spam? Unsolicited Commercial E-mail Research Six Month Report. Březen 2003. Citováno 18.4.2003.
http://www.cdt.org/speech/spam/030319spamreport.shtml

[33] DOČEKAL, Daniel. Spamming obsahuje lži, lži a lži. Pooh.cz, 30.4.2003, citováno 1.5.2003.
http://www.pooh.cz/a.asp?id=2004125&db=

[34] SYMANTEC CORPORATION. Průzkum provedený pro Symantec odhaluje rostoucí obavy z nevyžádané pošty. Tisková zpráva Symantec Corporation, 10.1.2003. Citováno 18.4.2003.
http://zive.cpress.cz/h/Info/Ar.asp?ARI=108935&CAI=

[35] SURVEY.NET. Internet Spam/UCE #1. Citováno 18.4.2003
http://www.survey.net/spam1r.htm

[36] HYMAN, Gretchen. Can the Spam, Say Office Workers. Internet Advertising Report, 12.2.2003. Citováno 18.4.2003.
http://www.internetnews.com/IAR/article.php/1583321

[37] HANZLÍČEK, Ladislav. Informační bezpečnost a analýza rizik – metodologie a nástroje. Diplomová práce, Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky, Katedra informačních technologií. 2000.

[38] DEFENSE INFORMATION SYSTEMS AGENCY. Information Systems Security for Managers. Prezentace. Citováno 25.4.2003.
http://nb.vse.cz/~gala/ib/mgr-crs.ppt

[39] DENÍKY BOHEMIA. Internet v prosinci navštívil rekordní počet uživatelů. 14.1.2003. Citováno 27.4.2003.
http://www.mojenoviny.cz/zpravy_z_cr/ekonomika/net030114.html

[40] WARD, Brian. Spam Statistics. Citováno 27.4.2003.
http://www.o--o.net/spam/index.php?exp=on

Terminologický slovník

Aktiva
Součást modelu ohrožení; to co je potřeba před spamem chránit.

Blacklist
Seznam odesílatelů/serverů, od kterých není přijímána elektronická pošta.

Cost/benefit analýza
Ekonomická analýza, která zjišťuje na základě nákladů a přínosů ekonomickou efektivnost projektu.

Dopady
Součást modelu ohrožení; škody způsobené hrozbami.

E-mailová konference, mailinglist
Aplikace, která rozešle zprávu odeslanou na jednu adresu na adresy všech přihlášených členů.

False positive
Legitimní zpráva, která je protiopatřením označena jako spam.

Filtrování
Označení některých zpráv jako spam podle určitých kritérií.

Freemail
Online služba umožňující vytvoření a používání e-mailové schránky zdarma.

Harvesting
Hromadné získávání e-mailových adres z veřejně dostupných zdrojů.

Hoax
Nepravdivá (většinou poplašná) zpráva řetězově šířená elektronickou poštou.

Hrozby
Součást modelu ohrožení; to co způsobuje ohrožení aktiv (spam).

ISP
Internet Service Provider, poskytovatel připojení k internetu.

Jednorázová adresa
E-mailová služba, která umožňuje vytvořit si libovolný počet e-mailových adres směřujících do stejné schránky.

Mailinglist
Viz e-mailová konference.

Maskování adres, munging
Uvádění e-mailových adres ve formátu čitelném pouze člověku, nikoliv robotům.

Munging
Viz maskování adres.

Open relay server
Servery, které umožňují třetí straně odesílat e-maily jiným subjektům na internetu.

Opt-in
Vyjádření žádosti uživatele o zasílání zpráv.

Opt-out
Vyjádření žádosti uživatele o zastavení zasílání zpráv.

Osobní údaj
Jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu. O osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času, úsilí či materiálních prostředků.

Protiopatření
Součást modelu ohrožení; opatření snižující zranitelnost systému.

Risk management
Součást procesu udržování rizik zabývající se zejména analýzou rizik, výběrem a implementací protiopatření.

Robot
Aplikace pro hromadné získávání adres.

Scam
E-mailové zprávy, pomocí kterých se odesílatel pokouší podvést adresáta.

Slovníkový útok
Získávání adres rozesíláním zkušebních zpráv na velké množství adres tvořených slovy ze slovníku na jednu doménu.

Spam
Nevyžádaná hromadná zpráva, která příjemci přináší zbytečné náklady. Také označuje celou předmětnou oblast.

Spam gang
Seskupení spammerů, kteří rozesílají spam ve velkém rozsahu.

Spamhaus
ISP, který toleruje rozesílání spamu ze svých serverů.

Spammer
Subjekt, který rozesílá nevyžádané hromadné zprávy.

Spamming
Rozesílání nevyžádaných hromadných zpráv.

Spamware
Specializovaný software sloužící k hromadnému odesílání nevyžádané pošty.

Usenet
Distribuovaný celosvětový diskusní systém, často nazývaný jako „news.“

Útok hrubou silou
Získávání adres rozesíláním zkušebních zpráv na velké množství náhodně vytvořených adres na jednu doménu.

Whitelist
Seznam odesílatelů/serverů, pouze od kterých je přijímána elektronická pošta.

Zranitelnosti
Součást modelu ohrožení; slabá místa, která mohou být využita k útoku na aktiva (poštovní server).

Přílohy

Příloha 1 – Příklad stížnosti na porušení zákona o regulaci reklamy

Toto je návrh možné stížnosti upravený ze stížnosti v kauze Tvujdum.cz zveřejněné na serveru Pooh.cz (*http://www.pooh.cz)*.

V _____, dne _____
Věc : Stížnost na porušení Zákona o regulaci reklamy

S ohledem na Zákon o regulaci reklamy (138/2002 sb), .§2, odst e) - ("šíření nevyžádané reklamy, pokud vede k výdajům adresáta nebo pokud jej obtěžuje"), tímto podávám stížnost na porušení tohoto zákona *doplnit osobu včetně kontaktních údajů, případně údajů z obchodního rejstříku*.

Ve dnech _____ až _____ jsem od *doplnit jméno spammera* obdržel nevyžádanou reklamu ve formě elektronické pošty zaslanou na mé adresy elektronické pošty. Tato nevyžádaná reklama mě nejenom obtěžuje, ale způsobila mi nesporné výdaje za internetové připojení.

Nevyžádaná reklama od šiřitele byla obdržena na tyto mé adresy: _____
_____
Ve všech obdržených případech s totožným obsahem (příklad jedné z konkrétních zpráv):

Doplnit text zprávy.

Žádám abych byl seznámen s výsledky šetření.

S pozdravem
Jméno a podpis.

Příloha 2 – Dotazník

Vytištěný dotazník naleznete na následujících listech.