evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERSITAS MASARYKIANA BRUNENSIS
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

NEVYŽÁDANÉ ZPRÁVY

INFORMAČNÍ BEZPEČNOST

13. 3. 2013 KISK FF MU

ZPRÁVY

- Komunikace = předávání informací
- Zprávy = předávání informací adresátům
- Push i pull, v reálném čase i offline, od známého i ne, hromadné i individuální, tradiční i elektronické – vše může být nevyžádané
- Zde omezeno na e-prostředí – komunikace jednou ze základních funkcí
- V tradičním prostředí podobné, ale ne tak snadné

E-KOMUNIKAČNÍ SLUŽBY

- Push:
  - E-MAIL
  - IM
  - VoIP
  - …
- Pull:
  - Diskuzní fóra
  - Webové stránky
  - …
- Sociální sítě = kombinace starších služeb (zprávy, IM, fóra, web…)

CHARAKTERISTIKY NEVYŽÁDANÝCH ZPRÁV

- Hromadně rozesílané, výjimečně cíleny na jednotlivce
- Lze odeslat velmi mnoho velmi rychle
- Základem sociální inženýrství (viz minulá přednáška)
- Příjemci (skoro nikdy) nepřináší užitek
- Stojí příjemce čas a technické prostředky

ČASTÉ PRVKY SDĚLENÍ (BARRETT, S. 69)

- PSYCHOLOGICKÝ NÁTLAK
- Neověřitelné citáty,
- Odkazy na známé společnosti, které ani nemusí mít nic společného s tématem zprávy,
- Mnoho velkých písmen, vykřičníků a přeškrtnutých S,
- Mnoho podrobných, ale pouze jednostranných informací,
- Řečnické otázky.

TYPY NEVYŽÁDANÝCH ZPRÁV

- Známý odesilatel
  - Řetězové zprávy
  - Hoax
- Neznámý odesilatel
  - Spam
  - Scam
- Typ ovlivňuje charakteristiky i možnosti ochrany

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERSITAS MASARYKIANA BRUNENSIS
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

ODESILATEL ZNÁMÝ

ŘETĚZOVÉ ZPRÁVY A HOAX

SHODNÉ RYSY

- Známý odesilatel zvyšuje důvěryhodnost
- Součástí žádost o přeposlání všem známým
- Přesvědčování: např. „Toto není hoax!“ „Nevěřil jsem, ale fakt funguje.“ „Můžeš mi věřit, jsem si jistý.“…

ŘETĚZOVÉ ZPRÁVY

- Spíš než řetěz je to lavina – jeden člověk rozešle mnoha svým známým
- Metody různé (strach, snaha pomoci, prospěch…)
- Častý útok na city (zvýšeno známostí odesilatele)

HOAX

- Někdy samostatně jindy druh řetězových zpráv
- = nevyžádaná poplašná zpráva, nezaložená na pravdě
- Snaha o důvěryhodnost zprávy (odesilatel důvěru má – je známý)
- Vystrašený si někdy sám ublíží (malware)

PŘÍKLADY

- Dopisy štěstí
- Černé sanitky
- Infikované injekční stříkačky (HIV) v metru a dětských hřištích
- Šmoulové na propagaci komunismu mezi dětmi
- Za 11. zářím Kanaďané – záviděli USA tak vysoké budovy

- Osvětimská lež

OCHRANA

- Rozeznání
  - Podle typických rysů
  - Databáze nevyžádaných zpráv, např. hoax.cz, v angličtině snopes.com, Don't Spread That Hoax! nebo HoaxSlayer
- Blokování slov (ne odesilatelů, ne učení)
- Dle § 209 TrZ není podvod – vyžadoval by úmyslné využití omylu jiného ve vlastní prospěch
- Hoax – při úmyslném způsobení znepokojení většího množství obyvatel určitého místa postižitelný dle § 357 Šíření poplašné zprávy TrZ

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERSITAS MASARYKIANA BRUNENSIS
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

ODESILATEL NEZNÁMÝ

SPAM, SCAM

PHISHING A PHARMING

SPOLEČNÉ CHARAKTERISTIKY

- Snahou užitek odesilateli na úkor příjemce
- Minimální náklady odesilatele – přesunuty na příjemce
- Získání kontaktů snadné (nákup, formuláře, harvesting…)
- U problémových odesíláno ze zombie
- Častý spoofing (důvěryhodnost, horší dohledání skutečného odesilatele)

SPAM

- Nevyžádaná zpráva od neznámého odesilatele, obvykle nabídka rozeslaná hromadně
- Obchodní, náboženská, politická…
- Dle výzkumů spam = desítky % dopravovaných e-zpráv (většina odfiltrována)
- „Spammerům stačí jedna odpověď (…) na dvacet milionů odeslaných zpráv“ (Přibyl – Sajrajt jménem spam)

SPAM - TERMINOLOGIE

- Termín v zákoně - § 7 zákona o některých službách informační společnosti – omezení na nevyžádané obchodní nabídky
- Běžně všechny nevyžádané nabídky rozesílané hromadně
- Možné kanály: E-MAIL, příspěvky a komentáře, webové stránky nebo blogy (splogy) i SMS, IM (spim) a VoIP (spit)
- Méně běžné + více cílené = důvěryhodnější
- Urážka konzervy – rozšiřuje se „Junk Mail“

SCAM

- Specifický spam
- Nevyžádaná zpráva nabízející příjemci pod nějakou podmínkou nevídaný finanční zisk
- Ve finále zisk u odesilatele
- Typické příklady: pyramidy, letadla, nigerijské dopisy, podvodné loterie

PHISHING A PHARMING

- Nevyžádané zprávy tvářící se jako vyžádané
- Terminologie užšího pojetí: phishing (e-mail), SMiShing (SMS), vishing (VoIP)
- Častý spoofing, zneužití Corporate Identity
- Cílem obvykle získání osobních informací (hl. OÚ, identifikační informace)
- Častá formulka „Neodpovídejte!“ - varování
- Nejznámější spojené s finančními institucemi, ale není podmínkou
- Oběť si své postavení nemusí uvědomit až do zneužití

PHISHING X PHARMING

- „Úlovková“ zpráva žádá poskytnutí informací skrz útočníkovo dílo (formulář, web i pop-up okno) – odhalitelné (URL)
- „Statisticky je (…) prokázáno, že na phishing zareaguje plných pět procent oslovených osob“ (Přibyl – Nebezpečí jménem phishing)

- „Vypěstování“ změny záznamů DNS u oběti umožní odkázat na správné URL s chybnou IP

OCHRANA

- Omezení sdělování kontaktních údajů
- Antispamový filtr dle adres, typických slov a spojení, Bayesovský filtr (vše + učení); především na e-maily, u jiných kanálů problém
- Antiphishingové nástroje
- Rozeznání, ideálně bez otevření
- SI – ověřování, nedůvěra…

MOŽNOSTI ZÁKONŮ ČR

- Zákon o některých službách informační společnosti
- Zde již využitelný § 209 Podvod TrZ
- Letadla a pyramidy (princip hry) trestné dle § 213 Provozování nepoctivých her a sázek TrZ

POUŽITÁ LITERATURA

- BARRET, Daniel, J. Bandité na informační dálnici. Kateřina Dufková. 1. vyd. Brno : Computer press, 1999. 235 s. ISBN 80-7226-167-3.
- BEDNÁŘ, Vojtěch. Hrozba jménem Spim. PC World [online]. 2007 [cit. 2011-03-16]. Dostupný z WWW: <http://pcworld.cz/ostatni/hrozba-jmenem-spim-5608>. ISSN 1210-1079.
- BITTO, Ondřej. Bojujte se spamem rychleji. Computer. 2008, č. 7, s. 78. ISSN 1210-8790.
- BusinessCenter.cz [online]. 2009 [cit. 2011-03-16]. Trestní zákoník. Dostupné z WWW: <http://business.center.cz/business/pravo/zakony/trestni-zakonik/>.
- CUNNINGHAM, Eleese, MARCASON, Wendy. Internet hoaxes : How to spot them and how to debunk them. Journal of the American Dietetic Association. 2001, vol. 101, is. 4, s. 460.
- DOLEŽEL, Michal. Tento e-mail pošli všem přátelům. Computer. 2005, č. 2, s. 82. ISSN 1210-8790.
- DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno : Computer Press, 2004. 190 s. ISBN 80-251-0106-1.
- GOLDSBOROUGH, Reid. What To Do About Internet Hoaxes. Tech Directions. 2006, vol. 66, is. 1, s. 10-11.
- KERA, Denisa. Všichni lžou všem, odhalte spiknutí. Computer. 2003, č. 15, s. 75. ISSN 1210-8790.
- KRÁL, Mojmír. Bezpečnost domácího počítače : Prakticky a názorně. 1. vyd. Praha : Grada, 2006. 334 s. ISBN 80-247-1408-6.
- NARAINE, Ryan. Spam surge linked to hackers. EWeek. 2006, vol. 23, is. 46, s. 11-12.
- PETERKA, Jiří. Jak pokračuje boj proti spammingu [online]. 2005 [cit. 2011-03-16]. Dostupný z WWW: <http://www.earchiv.cz/b05/b0321001.php3>.
- PETERKA, Jiří. W32/ExploreZip.worm : UŽ TO NENÍ HOAX [online]. 1999 [cit. 2011-03-16]. Dostupný z WWW: <http://www.earchiv.cz/anovinky/ai2287.php3>.
- PŘIBYL, Tomáš. Sajrajt jménem Spam. PC World. 2008, č. 3, s. 54-55. ISSN 1210-1079.
- PŘIBYL, Tomáš. VoIP a bezpečnost. PC World. 2006, č. 07-08. ISSN 1210-1079.
- SPRING, Tom. Mutující spam. PC World. 2006, č. 6, s. 70-71. ISSN 1210-1079.
- Zákon č. 480/2004 Sb., o některých službách informační společnosti [online]. c2000-2009 [cit. 2011-03-16]. Dostupný z WWW: <http://www.uoou.cz/index.php?l=cz&m=left&mid=11:01&u1=&u2>.

Děkuji za pozornost.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ