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

SOCIÁLNÍ INŽENÝRSTVÍ

INFORMAČNÍ BEZPEČNOST

27. 2. 2013 KISK FF MU

K ORGANIZACI…

- Podpisy k souhlasu s pomocí k disertaci
- Docházka v poznámkovém bloku

INFORMAČNÍ PROBLÉMY A BEZPEČNOST

1. Zjišťování informací
2. Útok
3. Ochrana

ZÍSKÁVÁNÍ INFORMACÍ K ÚTOKU

- Cílenější útok úspěšnější, ale náročnější X méně cílený – více oslovených
- Zneužitelné všechny informace, některé jako cesta k dalším
- Víc kroků => větší pravděpodobnost odhalení

LEGÁLNÍ ZDROJE

- Soubory, stránky, příspěvky… vyhledatelné
- Použitý HW k ukládání dat
- Hlavičky zpráv
- Programy za informace (freeware, shareware, adware…)
- …
- Samotná oběť

VYHLEDÁVÁNÍ ZNEUŽITELNÝCH OSOBNÍCH INFORMACÍ

JAK TO BYLO S OI?

- Osobní informace – pro širší vymezení než OÚ
- Většina problémů založena na osobních informacích
- Pro uživatele největší ohrožení přes jejich soukromí
- V komerčním prostředí obvykle kvalitní technické zajištění => útoky na lidi
- Člověk = vždy nejslabší článek zabezpečení
- Zneužitelné VŠECHNY informace o osobě, ale některé lépe, jiné jen v kombinaci
- Zneužitelné nejen osobní informace, ale např. i technické firemní… - ty nejsou cílem přednášky

O CO JDE ÚTOČNÍKŮM PŘEDEVŠÍM? (BARRETT, S. 31-32)

- E-mailová adresa – dobře vyhledatelná, zneužívána při většině útocích
- Skutečné jméno a příjmení, adresa, telefonní číslo apod. – často zveřejňovány
- Heslo k různým aplikacím – někdy lze také najít
- Informace o majetku, doba dovolené – někteří lidé zveřejňují, např. v diskuzích, sociálních sítích…
- Rodné číslo, čísla dokladů, kódy platebních karet, jméno matky za svobodna, informace o blízkých osobách apod. – silně zneužitelné

KATEGORIE ZOII (KRÁL, S. 100)

- červená – rodné číslo, číslo pojištění, identifikační čísla (PIN) účtů, rodné jméno matky, informace o zdravotním stavu, trestní rejstřík, podrobné informace o financích, cestovní plány, seznam předchozích zaměstnání, informace o rodině a přátelích vč. jejich telefonních čísel, e-mailových i skutečných adres, atp.
- oranžová (žlutá) – telefonní číslo, adresa, datum narození, stav, zaměstnavatel, vzdělání, e-mailová adresa, oblíbené nákupy, číslo kreditní karty, zájmy a koníčky, spolky a sdružení, navštívené webové stránky, apod.
- zelená – směrovací číslo, věk, přibližná výše platu, povolání, průzkumy veřejného mínění, atd., pokud tyto informace nejsou ve spojení s jinými, choulostivějšími údaji z předchozích skupin.

IDENTIFIKAČNÍ INFORMACE

- Nejlépe zneužitelné
- Identifikace v reálném prostředí: jméno, příjmení, datum narození, rodné číslo… (OÚ)
- Identifikace v elektronickém prostředí (nejčastěji znalostí): uživatelské jméno/číslo a heslo, e-mailová adresa, IP adresa...

ZÍSKÁVÁNÍ HESLA

1. Zkoušení předdefinovaných dvojic, prázdného hesla
2. Uhodnutí dle získaných OI (zapamatovatelné, příp. heslo jinde)
3. Lamače
    1. Slovníkový útok
    2. Útok hrubou silou

- čtvrtina (…) jako heslo používá nějaký pro ně snadno zapamatovatelný údaj, jako třeba datum jejich narození či nějakého výročí (Noska – Výzkum: Uživatelé hazardují se svými hesly k webovým službám; zde i mnoho dalších zajímavých výsledků)

ZÍSKÁVÁNÍ DALŠÍCH OI

- Přímo X nepřímo
- Cíleně X necíleně
- Legálně X nelegálně
- Eticky X neeticky
- Z aplikací, komunikace, malwaru, od uživatele…
- Viz SI
- Spojení s cílovou osobou

NĚKOLIK UKÁZEK ZDROJŮ

- AltaVista: www stránky s e-mailovou adresou
- IP adresa a doména: DNS nebo traceroute, zvláštní stránky s profily
- Sociální sítě (Facebook, Lidé…), virtuální světy (SL, WoW…), hry – všude, kde mají uživatelé profil

SNS A SLUŽBY SE SOCIÁLNÍMI PRVKY

SNS:

- Facebook
- Lidé
- Spolužáci
- Líbímseti
- Google+
- MySpace
- LinkedIn
- Twitter
- Badoo

Mobilní SNS:

- Foursquare
- Gowalla

Služby se sociálními prvky:

- YouTube

MOŽNOSTI NASTAVENÍ SOUKROMÍ

- Možnost být vyhledán
- Viditelnost kontaktních informací, informací o škole aj.
- Viditelnost zpráv, fotografií, videí

- Ukázka
  - Jméno: ukazkyprovyuku@seznam.cz
  - Heslo: 123456kisk

GOOGLE!

- Najde vše, ale musí se vědět jak, někdy lepší použít jiné metody (viz Long: Google hacking)
- Data publikovaná omylem, odstraněné informace přes archiv – doménové hledání a specifikace souboru
- Seznamy e-mailových adres nebo uživatelů
- Připojení na webkameru
- Nalezení hesel
- Atd.

PÁR TYPŮ VYHLEDÁVÁNÍ NA GOOGLU K VYZKOUŠENÍ

- Site: - lze přidat ke každému hledání pro cílení
- Intitle:index.of – adresáře ve stylu Apache
- Error OR warning – chybové zprávy často obsahují hodně technických informací
- Ligin OR logon – přihlašovací portály
- Username OR userid OR employee.ID OR „your username is“
- Password OR passcode OR „your password is“
- Admin OR administrator
- -ext:html –ext:htm –ext:shtml –ext:asp –ext:php – zahozením nejčastějších typů souborů lze najít zajímavější
- Inurl:temp OR inurl:tmp OR inurl:backup OR inurl:bak – záložní či dočasné soubory a adresáře
- Intranet OR help.desk – intranetové weby

ZNEUŽITELNÉ OI A E-OBCHODY

- Falešné či nedůvěryhodné obchody
  - Pořízení e-shopu snadné
  - SI pro získání OI – co s nimi dál?
- U mladých oblíbené technologie, služby, obsah (mobilní telefony, hudba, Instant Messaging nebo počítačové a internetové hry), za kterými mohou stát i známé společnosti, naplněné profily pro cílenou reklamu

OCHRANA OI

- Pozornost a zdravá nedůvěra (SI)
- Pozor na odpadky
- Aktualizace
- Nastavení prohlížeče
- Bezpečnostní aplikace
- Ochrana proti již popsaným ohrožením

ANONYMIZÉRY

- Pohyb po internetu s omezením sdělování informací
- Někteří provozovatelé se zavazují nezaznamenávat žádné aktivity uživatele
- Nutné doplnit vhodným chováním

AKTIVNÍ OCHRANA

- Aktivní boj proti zneužití OÚ – Zákon č. 101/2000 Sb., o ochraně osobních údajů + pomoc ÚOOÚ
- Velmi zajímavé stránky o zneužívání OI

POUŽITÁ LITERATURA

- BARRETT, Daniel J. *Bandité na informační dálnici*. Vyd. 1. Brno: Computer Press, 1999, 235 s. ISBN 80-722-6167-3.
- BITTO, Ondřej. Staňte se anonymními tichošlápky. *Computer*. 2006, č. 9, s. 85. ISSN 1210-8790.
- BOTT, Ed, SIECHERT, Carl. *Mistrovství v zabezpečení Microsoft Windows 2000 a XP*. 1. vyd. Brno: Computer Press, 2004. 696 s. ISBN 80-722-6878-3.
- ČEPIČKA, David a Sascha ZÄCH. Neprozraďte se!. *PC World* [online]. Praha: IDG Czech, 2006, č. 12 [cit. 2012-03-21]. ISSN 1210-1079. Dostupné z: http://www.pcworld.cz/pcw.nsf/507139fc8752e797c12568bb004a187b/6fa5c904dbaff2d7c1257275004ce35c?OpenDocument
- ČEPIČKA, David, et al. Co všechno o nás ví Microsoft. *PC World* [online]. Praha: IDG Czech, 2005, č. 5 [cit. 2012-03-21]. ISSN 1210-1079. Dostupné z: http://www.pcworldsecurity.cz/pcws.nsf/bezpecnost/26BD4B2686235E96C125708F0033D4D6
- ČEPIČKA, David. a Daniel BEHRENS. Objevte nové možnosti využívání internetových služeb. *PC World*. 2005, č. 5, s. 97-99. ISSN 1210-1079.

POUŽITÁ LITERATURA (2)

- JOHNSON, Dough. Staying Safe on the Read-Write Web. *Library Media Connection*. 2008, roč.. 26, č. 6, s. 48-52.
- CHESTER, Jeff a Kathryn MONTGOMERY. No Escape: Marketing to Kids in the Digital Age. *Multinational Monitor*. 2008, roč. 29, č. 1, s. 11-17.
- KILIÁN, Karel. Bezpečnost a anonymita na Internetu: Hesla a politika hesel. *1. PC Revue* [online]. 2002 [cit. 2012-03-21]. ISSN 1213-080X. Dostupné z: http://www.1pcrevue.cz/ak0420.htm
- KRÁL, Mojmír. *Bezpečnost domácího počítače: Prakticky a názorně*. 1. vyd. Praha: Grada, 2006. 334 s. ISBN 80-247-1408-6.
- MITNICK, Kevin. *Umění klamu*. Překlad Luděk Vašta. HELION S.A., 2003. 348 s. ISBN 83-7361-210-6.
- NOSKA, Martin. Výzkum: Uživatelé hazardují se svými hesly k webovým službám. *Computerworld* [online]. 14.10.10 [cit. 2012-03-21]. Dostupné z: http://computerworld.cz/bezpecnost/vyzkum-uzivatele-hazarduji-se-svymi-hesly-k-webovym-sluzbam-7882
- ZEMÁNEK, Jakub. Slabá místa Windows aneb jak se bránit hackerům. *Computer Media*, 2004. 156 s. ISBN 80-86686-11-6.

SOCIÁLNÍ INŽENÝRSTVÍ

PROČ SAMA OBĚŤ?

- „… každý čtenář už byl zmanipulován největšími sociotechnickými experty — svými rodiči. Ti našli způsoby jak zařídit, abychom "ve svém vlastním zájmu" dělali to, co je podle nich nejlepší. Rodiče jsou schopní všechno vysvětlit, stejně jako sociotechnici šikovně vymýšlejí věrohodné historky, důvody a argumenty, jen aby dosáhli svého. V důsledku takových zkušeností jsme se všichni stali náchylnými podlehnout manipulaci.“ (Mitnick, s. 27)

OBĚŤ JAKO ZDROJ

- Jistota, že jde o toho, kdo má být cílem
- Často jednoduché
- Stroj jedná dle instrukcí X člověk ovlivnitelný

REKLAMA

- SI ověřené z offline světa i legální
- „Americký ‘výzkum trhu‘, který se v posledních deseti letech velice rychle rozvinul, má silný totalitní sklon – sklon k sociálnímu inženýrství.“ (McLuhan, s. 20)
- Děti a mladí nejovlivnitelnější a napodobující – dospělí přes ně
- Publikace o úspěšné reklamě = o různých způsobech tlaku na zákazníka

SOCIÁLNÍ INŽENÝRSTVÍ

- Nejslabší článek zabezpečení IT = uživatel
- SI = podvod
- Cílem přimět uživatele udělat něco, co by jinak neudělal a co jej zřejmě poškodí
- Základem žádost ve správném kontextu

VÝHODY SI

- Uplatnitelné vždy:
  - Získávání i zneužití informací
  - Může být cíleno, ale nemusí
- Stačí minimum technických dovedností a znalostí
- Častá složka většiny útoků (zvyšuje úspěch), téměř jistě i do budoucna – proto zde podrobně

PŘEDPOKLADY

- Útočník: představivost, kreativita, umění vystupovat a komunikovat, sebedůvěra, rozumná drzost, instinkt, vyvolávající dobrý první dojem (příjemné vystupování)
- Oběti: hloupost, naivita, soucit, strach, hrdost, další běžné lidské vlastnosti; ale i inteligentního lze povést a manipulovat s ním
- Navázání kontaktu, nejčastěji e-mail (adresa se zjistí snadno)
- Útočník spoléhá na to, že oběť se cítí nevýznamná na to, aby byla cílem

PRŮBĚH

- Výběr a kontaktování vhodné oběti
- Útočník vždy něco požaduje (činnost, informace, peníze…)
- Metody přesvědčení oběti:
  - Očekávaná činnost
  - Útok na city
  - Lákavé nabídky
  - Vyvolání zvědavosti
  - Vybuzení osobního zájmu
  - Pocit viny
  - Snaha se odvděčit
  - Snaha napodobit jiné
  - …

ZVÝŠENÍ DŮVĚRYHODNOSTI

- Zneužití identity jiného, hl. autority pro oběť
- Zaštiťování se znalostí informací (např. z tzv. digitálních stop i odpadků), často považovaných za nevýznamné
- Očekávaný způsob komunikace
- Spoofing (e-mail, web), také forging (Barrett, s. 44)

ZHORŠENÍ OBRANY OBĚTI

- Nemožnost či minimalizace ověření
- Vyvolání stresu u oběti
  - Časový limit
  - Finanční postih
  - Jiné nebezpečí

TYPICKÉ PRVKY SOCIOTECHN. KOMUNIKACE

- Odmítnutí sdělit zpáteční číslo.
- Neobvyklá žádost.
- Ohánění se autoritou.
- Zdůrazňování naléhavosti záležitosti.
- Hrozba důsledky nevyhovění žádosti.
- Neochota volajícího odpovídat na dotazy.
- Zmiňování mnoha jmen.
- Komplimenty či pochlebování.
- Flirtování.

(Mitnick, s. 335)

OBRÁCENÁ SOCIOTECHNIKA

- Útočník kontaktuje oběť, ale nic po ní nechce, naopak na sebe odkáže jako na pomocníka při daném problému
- Problém je útočníkem vyvolán (příp. nejde o problém, ale normální záležitost)
- Oběť sama kontaktuje útočníka, necítí podezření

- Např. e-mail od poskytovatele připojení s popisem problému, který může nastat a nabídkou pomoci

FINÁLE – PODĚKOVÁNÍ OBĚTI

- Není nutné
- Může často oddálit odhalení – upokojí uživatele
- Je slušné poděkovat, když někdo udělá, co chceme… ☺

PŘÍKLADY

- Praní špinavých peněz z pohledu tn.cz
- Často zneužívány široce sledované záležitosti (katastrofy, fenomény,…)
- Letadla a pyramidy – může zahájit scam (13. 3.) i zveřejněná informace – viz můj mail
- Reklama a prodej – „speciální nabídka jen u nás, nejlevnější na trhu“ (pokud není běžně známá cena), prodej informací dostupných zdarma, slůvko „zdarma“ při nabídce zboží či služeb za úplatu

OBRANA

- ZDRAVÁ NEDŮVĚRA
  - Určitá důvěra nezbytná pro práci v e-prostředí, ale nic nepřehánět
  - Ověřování – nejlépe neelektronickou cestou (hlasovou, osobní)
  - Před poskytnutím informací si položit otázku: „Ublížilo by mi jejich prozrazení mému nepříteli?“
  - Je lepší se „ztrapnit“ než podlehnout sociotechnickému útoku
  - Nikdy nepomáhejte nikomu cizímu (i spolupracovník, spolužák …, kterého neznáte osobně)
  - Číst certifikáty, licenční podmínky, varování, potvrzení…

OBRANA (2)

- POZORNOST
  - Všímat si podrobností, ptát se na ně
  - Navrhovat alternativní (reálná) řešení – vyvede z míry
- NEBÝT POHODLNÝ
- Pokud víme, kde může být problém, víme kde omezit důvěru a zvýšit pozornost – VZDĚLÁVÁNÍ
- Čas od času ověřit, jaké informace o mé osobě/firmě jsou zveřejněny

DALŠÍ POMŮCKY

- Bezpečnostní strategie – nejčastěji ve firmách formou informační politiky (stanoví pravidla a postupy) => snaha o snížení vlivu psychiky na jednání
- Ve firmě nutné být vstřícný k zákazníkům, ale jen do stanovené míry (informační politika) a jen k tomu určení lidé
- Antiphishingové nástroje
- „Firmy, které provádějí penetrační testy bezpečnostních systémů, uvádějí, že pokusy nabourat se do počítačového systému zákazníka pomocí sociotechnických metod jsou skoro stoprocentně účinné. Technologická zabezpečení mohou takové útoky ztížit tím, že minimalizují účast lidí v rozhodovacím procesu.“ (Mitnick, s. 250)

OBRANA PŘI KONTAKTU E-MAILEM

- Zprávy od neznámých odesilatelů neotvírat
- Od známých odesilatelů kontrolovat konzistenci (styl i obsah)
- Předmět by měl odpovídat textu
- Zamyslet se nad tím, co odesilatel požaduje
- Nepoužívat odkazy ve zprávě (výjimkou mohou být potvrzovací e-maily doručené bezprostředně po činnosti uživatele)

OBRANA ÚTOKEM

- Mezinárodní řešení složité
- Podvod trestný podle § 209 TZ při zneužití omylu někoho jiného ve vlastní prospěch
- Dále podle toho, s čím je SI spojeno
- Letadla a pyramidy trestné podle § 213 Provozování nepoctivých her a sázek TZ
- Kontaktní informace samotné nejsou osobní údaje dle zákona 101/2000 Sb.

POUŽITÁ LITERATURA

- BARRET, Daniel, J. *Bandité na informační dálnici*. Kateřina Dufková. 1. vyd. Brno: Computer press, 1999. 235 s. ISBN 80-7226-167-3.
- ČESKO. Zákon č. 101 ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů České republiky*. 2000, částka 32, s. 1521-1532. Dostupný také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3420. ISSN 1211-1244.
- Trestní zákoník, ve znění pozdějších předpisů
- JAGODZIŃSKI, Marcin. *Hledá se: Kevin Mitnick* [online]. [cit. 2007-03-19]. Dostupné z: mitnick.helion.pl/about_k_mitnick.pdf
- MCLUHAN, Marshall. *Člověk, média a elektronická kultura : výbor z díla*. 1. vyd. Brno: JOTA, 2000. 424 s. ISBN 80-7217-128-6.
- MITNICK, Kevin. *Umění klamu*. Překlad Luděk Vašta. HELION S.A., 2003. 348 s. ISBN 83-7361-210-6.
- PŘIBYL, Tomáš. Ničivé vlny v Asii a počítačová kriminalita. *PC World Security*. 2005, č. 1, s. 44. ISSN 1214-794X.

Děkuji za pozornost.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ