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

ZABEZPEČENÍ

15. 5. 2013

KISK FF MU

INFORMAČNÍ BEZPEČNOST

- Problematická oblast, plno výjimek, bouřlivý vývoj, i u starého se pořád objevují nová problematická místa
- Ale přesto DOKONCE 3 jistoty:
  - 100% bezpečí neexistuje
  - nejvíc problémů si způsobí každý sám
  - prevence je vždy úspěšnější než represe
- Vzdělávání zde klíčové

SHRNUTÍ – ZABEZPEČENÍ

- Popsané platí nejen pro stolní počítače
- Možnosti na obou stranách pořád ve vývoji – zde jen základní a rámcové informace
- Útoky na informace či s využitím ICT mají mnoho podob, ale základní obranná opatření pořád stejná
- Nezaručí neprolomitelnou bezpečnost, ale zvýší pravděpodobnost přesunu útoku na snazší cíl (většina útoků zkouškových – příležitost dělá „zloděje“)

3 PILÍŘE PRO BEZPEČNOST

- Chování uživatele
- Možnosti běžného SW a HW vybavení
- Doplňková a specializovaná opatření

- + Jistota je jistota – vše zálohovat

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

CHOVÁNÍ UŽIVATELE

SOUHRN PRINCIPŮ

- Bezpečí při velkém počtu – už není ideální
- Zveřejňované informace – vždy si říct, zda to lze zneužít
- Ovládat se, myslet, ověřovat
- Pozor na problematické informace a zdroje (NNO)
- Stahování a instalace jen toho, co uživatel opravdu potřebuje (a po prověření)
- (Automatické) aktualizace a správné nastavení každého SW (vč. OS)

OBRANA PROTI SI

- ZDRAVÁ NEDŮVĚRA
  - Určitá důvěra nezbytná pro práci v e-prostředí, ale nic nepřehánět
  - Ověřování – nejlépe neelektronicky (hlasově, osobně)
  - Před poskytnutím informací si položit otázku: „Ublížilo by mi jejich prozrazení mému nepříteli?“
  - Je lepší se „ztrapnit“ než podlehnout
  - Nikdy nepomáhat nikomu cizímu (i spolupracovník, spolužák …, kterého neznáte osobně)

OBRANA PROTI SI (2)

- POZORNOST
  - Všímat si podrobností, ptát se na ně
  - Navrhovat alternativní (reálná) řešení – vyvede z míry
- NEBÝT POHODLNÝ
  - Číst certifikáty, licenční podmínky, varování, potvrzení…
  - Hesla v hlavě (ne na papíře či v prohlížeči)
- Se znalostí, kde může být problém, jasné, kde omezit důvěru a zvýšit pozornost – VZDĚLÁVÁNÍ
- Bezpečnostní strategie – nejčastěji ve firmách formou informační politiky

OCHRANA OSOBNÍCH INFORMACÍ

- Omezení sdělování kontaktních údajů, ale i dalších osobních informací
- Sledovat, co zveřejňují blízcí lidé a upozornit je, pokud to překročí mou hranici soukromí
- Čas od času ověřit, jaké informace zveřejněny o mé osobě/firmě
- Pozor na odpadky

E-MAILY

- Opatrná práce s e-maily a přílohami – rozhodování:
  1. Dle odesilatele
  2. Dle obsahu
  3. Problematické hned smazat
- Zprávy od neznámých odesilatelů neotvírat
- Od známých kontrolovat konzistenci (styl i obsah)
- Předmět by měl odpovídat textu
- Zamyslet se nad tím, co odesilatel požaduje
- Nepoužívat odkazy ve zprávě (výjimkou potvrzovací e-maily doručené ihned po činnosti)
- Rozeznání nevyžádané zprávy podle typických rysů, příp. databáze (v prevenci), ideálně bez otevření

NNO (I KYBERŠIKANA)

- Zájem blízkých lidí, všímání si chování
- Omezování setkání dětí s NNO – zájem a aktivita rodičů i jiných (učitelka nechala děti dívat se na agresivní video, protože „budou hodné“)
- Není vhodné úplné zamezení přístupu – tím větší šok při nevyhnutelném setkání
- Vysvětlit neoprávněnost argumentů (extremistických a náboženských skupin, ale i pro hájení porušení AZ)

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

BĚŽNÉ VYBAVENÍ

MOŽNOSTI BĚŽNÉHO VYBAVENÍ

- (automatické) aktualizace u všeho SW, vč. OS
- Neustupovat pohodlnosti na úkor bezpečnosti, např. pamatováním hesel
- Správné nastavení webového prohlížeče (soukromí, zóny obsahu, Cookies, ActiveX, vyskakovací okna…)

OS (WIN PRO BĚŽNOST)

- Uživatelské účty mohou hodně pomoci, u vyšších verzí upraveno UAC
  - Win Vista: 0/1 + výjimky
  - Win 7: 4 úrovně + výjimky
- Bezpečné přihlášení (Ctrl+Alt+Del)
- Bezpečná hesla lze někdy vynutit (např. složitost, stáří, délka, historie hesel)
- Zaheslovaný spořič, max. po 10 minutách

FILTROVÁNÍ OBSAHU (NNO, SPAM ATD.)

- Backlist – nespolehlivé
- Whitelist – silně omezující
- Nastavení indikátorů, hl. slov a spojení, ne vždy spolehlivé (hodnotí pravděpodobnost)
- Služby hodnocení ručně důvěryhodným zdrojem/komunitou – nezávislé na jazyku, ale limitovaný počet ohodnocených zdrojů, často vzniká whitelist/blacklist

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

BEZPEČNOSTNÍ APLIKACE

VÝZKUM STEGANOS (2008)

- V USA a GB
- 13 % dotázaných nepoužívá antivir a dalších 9 % si není jisto
- Firewall nepoužívá také 13 % a jistých si není 21 % dotázaných
- 52 % účastníků nevědělo, jaké mají nastavení pro ochranu soukromí

BEZPEČNOSTNÍ APLIKACE

- Dnes by mělo být běžné vybavení
  - Antivir
  - Antirootkit
  - Antispyware
  - Firewall
  - Antispam
- (rodičovská ochrana)
- Antispam: whitelist, blacklist, Bayesovo filtrování; hl. spojené s e-maily
- Antiphishingové nástroje (možné v bezpečnostním balíku, plugin, protokol napojený na vyhledávač…)

ANTI-MALWARY

- Antiviry = první bezpečnostní aplikace
- Od té doby se změnily ony i hrozby, proti kterým stojí
- Velmi různorodé (specializované X všeobecné, různé techniky, nástroje, nastavení…)
- Obecně chrání nejen proti virům
- Specializované – antirootkit, antispyware

FUNKCE „ANTIMALWARU“

- Porovnávání signatur (nejstarší)
- Heuristická analýza (najde i nový malware)
- Analýza chování
- Kontrola integrity
- Sledování veškeré komunikace (hl. e-mailů a příloh)
- Rezidentní a nerezidentní ochrana
- Automatické aktualizace

FIREWALL

- Dělí chráněnou síť od nechráněné
- Ochrana proti nechtěnému transferu dat
- Filtruje pakety
- Uzavírá porty a nepoužívané služby
- Může odhalit skenování portů
- Nové funkce IDS (Intrusion Detection System) a IPS (Intrusion Prevention System): poznají vnější síťové útoky, kontrola integrity či analýza chování

ANONYMIZÉRY

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

Děkuji za pozornost.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ