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

BEZPEČNÉ CHOVÁNÍ A AUTENTIZACE

INFORMAČNÍ BEZPEČNOST

KISK FF MU

INFORMAČNÍ BEZPEČNOST

- Plno výjimek, bouřlivý vývoj, i u starého stále nové problémy
- Přesto DOKONCE 3 jistoty:
  - 100% bezpečí neexistuje
  - nejvíc problémů si způsobí každý sám
  - prevence je vždy úspěšnější než represe
- Vzdělávání zde klíčové

VAŠE ZDROJE

- Co jsme neprobrali?
- Jaká bezpečnostní opatření v chování vyplynula z různých zpracovaných materiálů?
- Jakým problémům to předchází/co to řeší?
- Které z řešených problémů jsou do jaké míry spojené s ochranou na úrovní chování/technické?

SOUHRN PRINCIPŮ

- Ovládat se, myslet, ověřovat (ne elektronicky)
- Zdravá nedůvěra, pozornost (drobnosti), nebýt pohodlný (číst, nezaznamenávat…)
- Pozor na NNO (zdroje i informace)
  - Psychické důsledky
  - Zájem blízkých, důvěra
  - Blokování problematické (slabiny + šok nepřipravených)
- Stahování a instalace nezbytného a po prověření
- Vzdělávání (problémy i řešení), LLL
- Bezpečnostní strategie

OCHRANA OI

- Zveřejňované informace – lze zneužít?
- Omezení sdělování kontaktů i dalších OI
- Pravidelný egosurfing, vč. informací zveřejněných blízkými => řešení s oprávněnými
- Pozor na odpadky

E-MAILY

- Rozhodování:
  1. Dle odesilatele (od neznámých neotvírat)
  2. Dle obsahu (konzistence, požadavky, odkazy)
  3. Problematické hned smazat
- Rozeznání nevyžádané dle typických rysů, příp. databáze, ideálně bez otevření

OBRANA ÚTOKEM

- Mezinárodní řešení složité (např. svoboda projevu)
- Proti zneužití OÚ z. č. 101/2000 Sb., o ochraně osobních údajů + pomoc ÚOOÚ => nepoužitelné pro kontakty
- Technické útoky a TrZ:
  - § 230-§ 232 jakýkoli úmyslný zásah do IS, chrání nosič i obsah
  - § 209 podvod při zneužití omylu někoho jiného ve vlastní prospěch
  - § 352 Násilí proti skupině obyvatelů a proti jednotlivci, § 353 Nebezpečné vyhrožování, § 354 Nebezpečné pronásledování
  - § 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob, § 356 Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod
  - § 357 Šíření poplašné zprávy
  - § 403 Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka, § 404 Projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka, § 405 Popírání, zpochybňování, schvalování a ospravedlňování genocidia

AUTENTIZACE + AUTORIZACE

- Identifikace v elektronickém prostředí
  - E-mailová adresa
  - Heslo k různým aplikacím – jak prolomit? => jak má vypadat?
- Ukázka nastavení soukromí na FB:
  - Jméno: ukazkyprovyuku@seznam.cz
  - Heslo: 123456kisk

AUTENTIZACE

- Základ bezpečnosti všeho personalizovaného, vč. dat, činností…
- Zařízení, uživatele
- FIDIS (Future of IDentity in the Information Society) – Something you: know, have, are, (do, are assigned to)
- X autorizace
- Dvou- a třífaktorová

ZÁSADY BEZPEČNÉHO HESLA

MUSÍ BÝT:

- Aa1*
- 8/12 znaků
- Změna max. za 90 dní

NESMÍ BÝT:

- Běžné slovo
- Znakové řady
- Přednastavené
- Opakující
- Zapsáno
- Nikomu sděleno

JAK S TÍM?

- Útoky: uhodnutí, lamače
- Pomůcky: algoritmus tvorby, správce, úrovně politiky, HW doplňky
- Vyzkoušíme?

PŘÍKLADY V PRAXI

- Prostá autentizace heslem: SMTP, POP3 a IMAP protokoly pro připojování k e-mailovým serverům, ICQ pro komunikaci přes Internet
- Tokeny: platební karty, autentizační kalkulátor, USB tokeny, telefony (přihlášení na FB)
- Biometriky: přihlašování k mobilním zařízením otiskem prstu, rozpoznáním obličeje
- Grafická hesla: gesta, body na obrázku (Win8/10)

ŠIFROVÁNÍ

- E-mailů, dokumentů…, ale i přenos dat (někdy na rozhodnutí uživatele)
- Ochrana proti odposlechu, krádeži…
- Stává se povinným – e-podpis, GDPR

NÁVRAT K PROBLÉMŮM

- IB pro každého jiná – skupiny
- Téma: jaká bezpečnostní opatření by měl daný člověk znát a využívat?
  - Dítě 12 let
  - Dospívající 20 let
  - Dospělý 30 let
  - Rodič na rodičovské dovolené (batole a předškolák)
  - Senior 65 let
- Postup: třífázový rozhovor => poster k prezentaci

TŘÍFÁZOVÝ ROZHOVOR

- **Jak se chránit vlastním chováním?**
- Trojice (A – B – C)
  - A klade otázky (rozhovor)
  - B odpovídá na otázky
  - C zapisuje klíčové, na konci přečte pro nezkreslení
- Po 5 min. střídání rolí, pak ještě jednou (každý v každé roli)
- Otázky lze opakovat, ale snaha najít co nejvíc možností (i dílčích, např. variace)
- Kdo daný postup zapsal, představí (dáme vše dohromady)

MOŽNÉ OTÁZKY - JAK SE ZABEZPEČIT?

- Co zveřejňovat/komunikovat přes internet?
- Jak se vyhnout útokům se sociálním inženýrstvím?
- Jak hodnotit důvěryhodnost v e-prostředí?
- Jak řídit nastavení pro ochranu soukromí? V jakých službách?
- Jakému obsahu se vyhýbat? Kdo? Proč?
- Jak nastavit autentizaci a autorizaci? Kde?
- Sledovat aktuální hrozby? Kde? Jak?
- Je důležitější pohodlí nebo bezpečí? Kde je hranice?
- Jsou nějaké zákonné možnosti pro ochranu/obranu?

POUŽITÁ LITERATURA

- BARRET, Daniel, J. Bandité na informační dálnici. Kateřina Dufková. 1. vyd. Brno: Computer press, 1999. 235 s. ISBN 80-7226-167-3.
- DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno : Computer Press, 2004. 190 s. ISBN 80-251-0106-1.
- JOHNSON, Dough. Staying Safe on the Read-Write Web. Library Media Connection. 2008, roč.. 26, č. 6, s. 48-52.
- KRÁL, Mojmír. Bezpečnost domácího počítače: Prakticky a názorně. 1. vyd. Praha: Grada, 2006. 334 s. ISBN 80-247-1408-6.
- POŽÁR, Josef. Informační bezpečnost. Plzeň: Aleš Čeněk, 2005, 309 s. Vysokoškolská učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.
- Trestní zákoník, v platném znění

DĚKUJI ZA POZORNOST.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ