ZABEZPEČENÍ INFORMACÍ A SÍTÍ

Přehled základních znalostí z oblasti informační a síťové bezpečnosti

Školitel: Jiří Stibor

Cíle

V tomto kurzu jsou prezentovány základy informační a síťové bezpečnosti:

- Jak lze informační a síťovou bezpečnost zajistit,
- Jak chránit osobní počítač
- Jak zmírnit bezpečnostní hrozby různých typů

Dále zde studenti naleznou základní informace týkající se síťové bezpečnosti:

- bezpečnostní protokoly
- firewallů
- systémů pro odhalování průniku
- standardních řešení pro zajištění bezpečnosti bezdrátových sítí

Literatura

1) Bruce Schneier: Applied Cryptography. John Kiley & Sons, Inc., New York, 1994
2) William Stallings: Cryptography and Network Security. Principles and Practices. Prentice Hall, New Jersey, 2003
3) Vesna Hassler: Security fundamentals for E-Commerce. Artech House, Boston, 2001
4) Rolf Oppliger: Internet and Intranet Security. Artech House, Boston, 2002
5) Michael Sikorski, Andrew Honig: Practical Malware Analysis, The Hands-On Guide to Dissecting Malicious Software. No Starch Press, February 2012
6) Michael Goodrich,Roberto Tamassia: Introduction to Computer Security, 2010
7) John R. Vacca: Computer and Information Security Handbook (Morgan Kaufmann Series in Computer Security), 2009
8) Jason Andress: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Elsevier, 2011

Rozdělení bezpečnosti

Informační bezpečnost se nezabývá jen šířením virů, ochranou před hackery nebo potíráním Spamu v emailech. Patří k ní i práce se zaměstnanci a managementem. Je potřeba jejich uvědomění si současných hrozeb, jejich seznamování s metodami ochrany informací a systémů.

Rozlišujeme:

- informační bezpečnost
- počítačovou bezpečnost
- síťovou bezpečnost

Informační bezpečnost

Informační bezpečnost znamená ochranu informací a informačních systémů před neoprávněným přístupem, využíváním, vyzrazením, narušením, pozměňováním, prohlížením, sledováním, zaznamenáváním či zničením.

Informační bezpečnost se zabývá důvěrností, integritou a dostupností dat, bez ohledu na jejich formu: elektronickou, tištěnou, či jinou.

Počítačová bezpečnost

Jako počítačová bezpečnost se společně označuje celá škála nástrojů určených k ochraně zpracovávaných a ukládaných dat a k boji proti záměrům hackerů.

Počítačová bezpečnost se může zaměřovat na zajištění dostupnosti a správné funkce počítačového systému, bez ohledu na informace v něm uložené nebo jím zpracované.

Síťová bezpečnost

Síťová bezpečnost je taktéž společné označení pro množinu nástrojů určených k ochraně dat během jejich přenosu.

Síťová bezpečnost se týká ochrany dat během jejich přenosu.

Příčiny nedostatečné bezpečnosti

Data lze snadno kopírovat, přenášet, pozměnit nebo zničit. Místo činu bývá velmi nepřehledné: nejsou zde žádné stopy, identifikace pachatelů je téměř nemožná.

Právní rámec navíc neobsahuje vhodná ustanovení, která by tento typ trestné činnosti dostatečně postihovala.

Na Internetu se vše odehrává v reálném čase, tento typ trestné činnosti dílem okamžiku.

Slabá místa umožňující porušení bezpečnosti

Je potřeba soustředit se na řešitelné oblasti.

Máme tři kategorie slabých míst:

- Slabá místa technologie
- Slabá místa v pravidlech
- Slabá místa v konfiguraci

Slabá místa technologie

Každá technologie má svá slabá či zranitelná místa, ať už známá, nebo neznámá, která může dostatečně motivovaný útočník zneužít.

Například:

- Internetové protokoly nebyly navrženy s ohledem na bezpečnost.
- Počítač a síťové operační systémy– každý *operační systém (OS)* má určitá zranitelná místa, která je nutno ošetřit pomocí oprav (tzv. záplat), aktualizací a doporučených postupů.
- Slabá místa síťových prvků. Síťové prvky či zařízení mají zranitelná místa (bezpečnostní díry). Opravy a aktualizace operačního systému instalovány a doporučené postupy aplikovány jakmile jsou k dispozici

Slabá místa v pravidlech

Jako slabá místa v pravidlech souhrnně označujeme opatření přijatá firmou vedoucí bezděčně, avšak nevyhnutelně k ohrožení bezpečnosti síťového systému.

Například:

- **Neexistují psaná bezpečnostní pravidla**. V praxi jsou naplňovány formou „best-effort“.
- **Neexistuje plán obnovy po havárii**. Do boje se musí proti síťovému útoku zapojit ti zaměstnanci, kteří jsou právě nablízku.
- **Neexistují pravidla pro přidávání a změny softwaru a hardwaru**. Neschválený bezdrátového AP může otevřít vrata sítě. Neznámý spořič obrazovky může data pro neznámého útočníka.
- **Neprovádí se bezpečnostní kontrola.** Nejhorším případem je, když ani závažné ztráty nejsou rozpoznány a může k nim docházet i nadále.
- **Zaměstnanecká politika.** Může se stát že noví, nedostatečně prověření a nezkušení zaměstnanci dostávají do funkcí, k nimž patří rozhodovací pravomoci a odpovědnost.
- **Vnitřní politika.** Hovoříme o syndromu „jsme tu všichni jako rodina“. I některé z nejlepších rodin mají zloděje. Podobně i rivalita, pomlouvání, boje o moc mohou zapříčinit bezpečnostní rizika, případně odvést pozornost.

Slabá místa v konfiguraci

Mnohá síťová zařízení mají výchozí nastavení, které jsou volena s ohledem na maximální výkonnost nebo snadnou instalaci, avšak bez ohledu na bezpečnostní rizika. Není-li při jejich instalaci věnována náležitá pozornost úpravě těchto nastavení, mohou následně nastat vážné problémy.

Například:

- Neefektivní seznamy přístupových pravidel, které nedokáží blokovat určený provoz.
- Výchozí, zcela chybějící nebo stará hesla.
- Nepotřebné porty nebo služby, které jsou ponechány aktivní.
- Uživatelská jména a hesla zasílaná jako otevřený text.
- Nedostatečně chráněný vzdálený přístup.

Klasifikace útoků

Bezpečnostní útoky můžeme popsat jako systematickou činností zacílenou na snížení nebo narušení bezpečnosti. Z tohoto hlediska je možno útok definovat jako systematickou hrozbu způsobenou nějakou entitou, a to uměle, úmyslně a inteligentně.

Nejčastější druhy útoků:

- **Sociální inženýrství**
- **Zlomyslná volání**
- **Útoky typu odmítnutí služby**
- **Útoky založené na protokolech**
- **Útoky na hostitelské počítače**
- **Odhadování hesel**
- **Odposlouchání všeho druhu**

Rozdělujeme je do dvou hlavní kategorií:

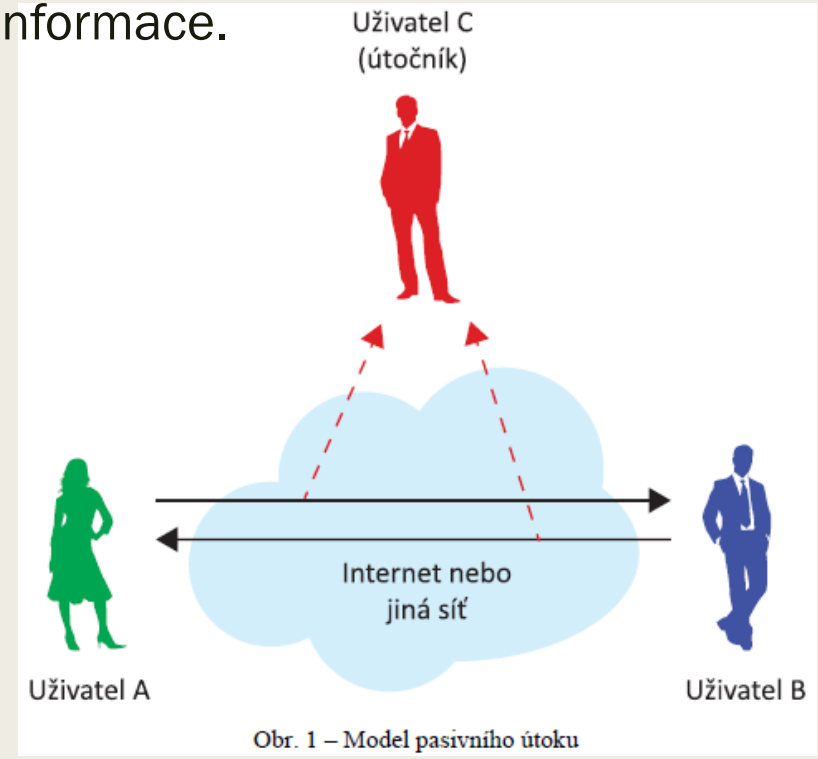
- Pasivní útoky
- Aktivní útoky

Pasivní útoky

Cílem pasivních útoků je získat nebo využít informace ze systému, nemají však vliv na systémové prostředky. Při pasivním útoku útočník pouze monitoruje komunikační kanál a ohrožuje důvěrnost dat. Povaha pasivních útoků tedy spočívá v odposlouchávání či monitorování přenosu s cílem získat přenášené informace.

Rozeznáváme dva typy pasivních útoků:

- Odposlouchávání
- Analýza provozu



Obr. 1 – Model pasivního útoku

Aktivní útoky

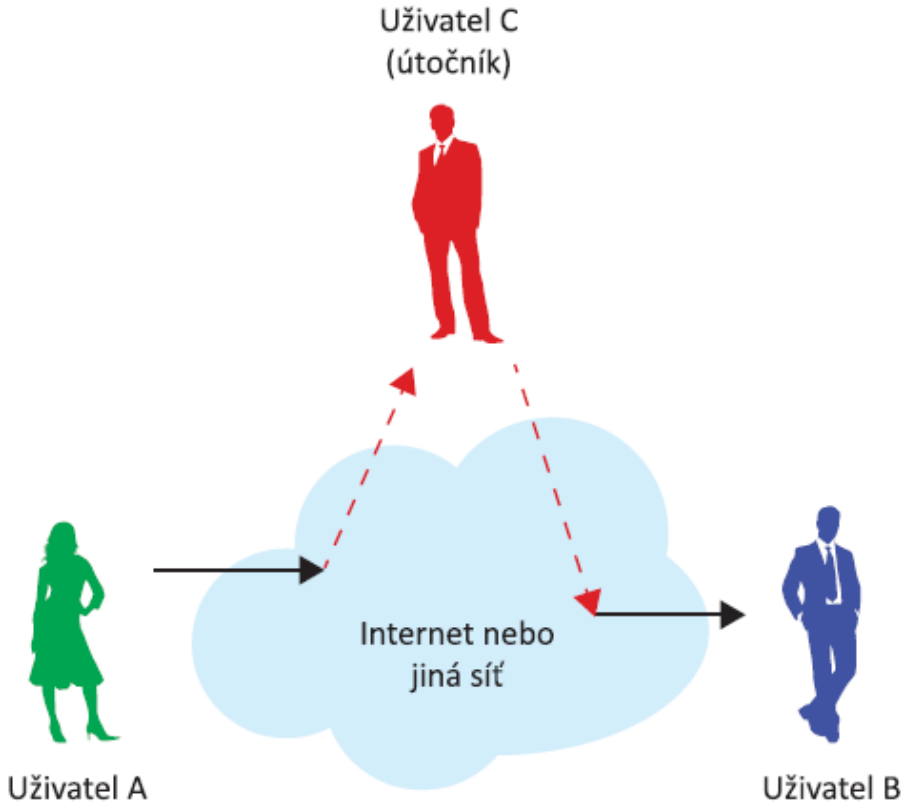
Aktivní útoky se pokoušejí měnit systémové prostředky nebo ovlivnit jejich funkčnost. Při tomto typu útoku se útočník snaží data přenášená příslušným kanálem odstranit, přidat nebo jinak měnit. Aktivní útočník ohrožuje integritu dat, jakož i autentizaci a důvěrnost.

Součástí aktivních útoků je nějaká změna datového toku nebo vytvoření toku falešného.

Rozeznáváme šest kategorií aktivních útoků:

- **Maškaráda**
- **Přehrání zprávy**
- **Pozměnění zprávy**
- **Člověk uprostřed** (MitM – Man in the Middle)
- **Odepření služby** (DoS – Denial of Service) **a Distribuované odepření služby** (DDoS – Distributed DoS)
- **Trvalá významná hrozba** (APT – Advanced Permanent Threat)

Aktivní útoky



Obr. 2 – Aktivní útok s pozměněním zprávy

Útočníci

Útočník či narušitel je osoba, která získá, případně se snaží získat větší než přidělená práva nebo neoprávněný přístup k informačnímu systému.

Útočníky můžeme rozdělit podle mnoha kritérií. Následující klasifikace je nejpoužívanější. Rozdělujeme podle:

- Umístění útočníka vzhledem k napadenému systému
  - *Vnitřní útočník – **insider***
  - *Vnější útočník – **outsider***
- Úrovně útoku
  - *Amatéři*
  - *Profesionnálové*

Útočníci - pokračování

- Cíle útočníka
  - ***Hackeři*** *– odborník vyhledávající zranitelná místa a bezpečnostní díry za účelem jejich zajištění*
  - ***Crackeři*** *– obecně odborník překonávající ochranu z neetických důvodů. (Peníze, pomsta, zdiskreditování konkurence, zablokování činnosti…)*
  - ***Scriptkiddies*** *- uživatele s nízkou úrovní dovedností v oblasti IT. Ke svým útokům využívají skripty obsahující kódy zaměřené na zneužívání zranitelných míst informačních systémů, aniž by znali hlubší podstatu jejich fungování. Dopady jejich činnosti jsou však obvykle závažné. Jedná se o nejčastější a nejnebezpečnější typ útoků.*
  - *A další*

Jak se lze chránit – obecná doporučení

- Používejte silná hesla
- Vždy používejte antivirový program
- Vždy změňte výchozí nastavení
- Používejte firewall
- Neotvírejte neznámé přílohy e-mailů
- Nespouštějte programy neznámého původu
- Bez prodlení aktualizujte všechny aplikace i operační systém
- Když počítač nepoužíváte, vypněte jej nebo odpojte od sítě
- Pravidelně zálohujte důležitá data a vytvořte si spouštěcí disk

Silná hesla

- Hesla jsou klíčem k vaší síti, a proto byste je měli co nejlépe chránit. Firewally a systémy detekce průniku jsou k ničemu, pokud dojde k vyzrazení vašich hesel.
- Silné heslo je takové, které nelze nalézt v žádném slovníku – českém, anglickém ani jiném, tedy, heslo, které není snadné uhodnout. Je samozřejmě těžší odhadnout nebo prolomit delší hesla nežli krátká.
- Pokud má řadový uživatel podezření, že heslo bylo zcizeno nebo vyzrazeno, měl by své heslo okamžitě změnit a oznámit událost tomu, kdo ve firmě odpovídá za bezpečnost.

Administrátorská hesla

Superuživatelská a administrátorská hesla jsou pro útočníka jako klíče od království. Správci systému s právy superuživatele (root) – tedy bez jakýchkoli omezení přístupu a s možností provádět jakékoli změny – by proto měli mít ta nejsložitější hesla a nejpřísnější pravidla pro jejich změny a opětovné použití. Doporučuje se dodržování následujících pokynů:

- Zapište si všechna administrátorská hesla a zamkněte je do trezoru: I když se pak stane, že správce je nedostupný, není heslo nenávratně ztraceno.
- Změňte VŠECHNA uživatelská hesla, jestliže existuje podezření na vyzrazení hesla administrátorského: Nelze zaručit, že nebyla zcizena všechna hesla, pokud se neznámá osoba zmocnila hesla superuživatele nebo administrátora.

Pravidla silných hesel

- **Použijte nesmyslnou kombinaci písmen:** Nejlepší hesla jsou zcela nesmyslná. Vezmeme-li například větu „Neočekávejte ode mne dokonalé chování a zářivý úsměv“ a použijeme-li jen první znak každého slova, dostaneme heslo nomdcazu.
- **Smíchejte velká a malá písmena:** Heslo by mělo obsahovat velké písmeno někde jinde než na začátku, a mělo by se v něm vyskytovat také číslo.
- **Nepoužívejte jako heslo posloupnost písmen, která jsou na klávesnici za sebou:** Je třeba vyhýbat se používání takových hesel, jako je QWERTY, 12345678, nebo asdfghj. když vypadají nesmyslně, jsou tvořena podle jasného vzoru po sobě jdoucích znaků na klávesnici počítače, a pro crackera není problém prolomit je za několik sekund.
- **Delší hesla jsou lepší:** Délka hesla by měla být alespoň 8 znaků.

Pravidla silných hesel - pokračování

- **Hesla byste měli pravidelně měnit**: Dokonce i ta nejlepší hesla by měla být pravidelně měněna (řekněme po 60 dnech), neboť při dlouhodobém používání se zvyšuje riziko prolomení. Řada operačních systémů umožňuje nastavit toto pravidlo pro všechny uživatele. Uživatelům se to nejspíš bude zdát nepohodlné, ale jde o zajištění bezpečnosti.
- **Vymýšlejte nová hesla namísto opakovaného užívání starých**: Uživatel by neměl znovu použít stejné heslo po dobu alespoň jednoho roku, nebo dokonce 18 měsíců.
- **Zacházejte s hesly jako s přísně tajnou informací**: Všechna hesla by měla být chráněna, nikoli sdělována druhým! Řada uživatelů si píše hesla na poznámkové lístečky nalepené na počítač nebo si je dává pod klávesnici. Tím ale nikoho neošálí!

Shrnutí

Dnes jsme se nejprve seznámili s několika důležitými pojmy, jimiž jsou informační bezpečnost, počítačová bezpečnost a síťová bezpečnost, a uvedli jsme si, jaké jsou mezi nimi rozdíly. Poté jsme si uvedli některé příčiny nedostatečného zabezpečení informací a roztřídili si typy bezpečnostních útoků a útočníků podle různých hledisek. Nakonec jsme probrali oddíl shrnující doporučení, jak mohou domácí uživatelé zlepšit ochranu svých systémů.