

Identifikátor materiálu: **ICT-2-02**

Předmět	Informační a komunikační technologie
Téma materiálu	Bezpečnost dat 2
Autor	Ing. Bohuslav Nepovím
Anotace	Student si procvičí / osvojí narušení bezpečnosti.
Druh učebního materiálu	Prezentace (Výklad / Test)
Typ vzdělávání	Střední škola / SOU
Ročník	1. – 3.
Datum vytvoření	Prosinec 2012

Informační a komunikační technologie

Bezpečnost dat 2

Narušení bezpečnosti

Moderní společnost je čím dál tím více závislá na přenosu, třídění a ukládání informací. Informace se stávají zbožím. Zároveň s tím narůstá složitost systémů, které přenos a zpracování informací umožňují, a také se zvyšuje míra jejich integrace a provázanosti. Jedním z projevů tohoto vývoje je i existence celosvětové datové sítě Internetu. Čím dál tím více se tedy stává problémem ne to, jak informace získat nebo dopravit na potřebné místo, ale jak zajistit, aby dotyčné informace měli včas k dispozici ti, kterým jsou určeny (např. ti, kteří si za ně zaplatili), a naopak, aby se nedostaly k těm, před kterými mají zůstat utajeny.

Narušení bezpečnosti se dá provést několika způsoby (vydávání se za jinou osobu a zneužití jejích privilegií; změnou práv ostatních osob; bráněním uživatelům legitimně komunikovat...a mnoho dalších)

Druhy útoků

Útok, neboli bezpečnostní incident je buď úmyslné využití zranitelného místa ke způsobení škod (ztrát), nebo neúmyslné uskutečnění akce, jejíž výsledkem je škoda.

Útoky lze provádět

- přerušením: útok na dostupnost (ztráta, znepřístupnění, vymazání dat, porucha periferie....)
- odposlechem: útok na důvěrnost (okopírování dat, programu...)
- změnou: útok na integritu (změna mailu, změna uložených dat, přidání funkce do programu...)
- přidáním hodnoty: útok na integritu nebo na autenticitu (neautorizovaná strana něco vytvoří: podvržení transakce, dodání falešných dat, poslání mailu pod jiným jménem)

Útoky lze také dělit na:

- s velkou škodou (tyto útoky mohou mít pro organizaci katastrofický dopad případně i krach)
- s malou škodou (škody nejsou tak významné)

nebo také:

- útoky na HW
- útoky na SW
- útoky na data

Útočník

Důležité je třeba si uvědomit, kdo může útočit. Útočník může být vnější/vnitřní a podle znalostí a dovedností a vybavenosti rozeznáváme útočníky:

- slabé síly (amatéři, náhodní útočníci)
- střední síly (hackeři)
- velké síly (počítačové profesionálové „zločinci“)

Zranitelné místo

Je slabina informačního systému (IS), která se dá využít ke způsobení škod nebo ztrát útokem na informační systém. Podstata zranitelného místa může být:

- fyzická (umístění PC/IS na místě, které je dostupné vandalismu, sabotáži....)
- přírodní (záplava, požár, tajfun...)
- v HW nebo SW
- v lidském faktoru (největší zranitelnost ze všech variant)

Riziko

Je pravděpodobnost využití zranitelného místa.

Sociální inženýrství

Sociální inženýrství je moderní metoda počítačového útoku na nejslabší článek těchto systémů, a tím je člověk. Psychologie a umění ovládat lidi, neboli využívání lidských slabin v jednání, jsou nejmocnější zbraní sociotechnika. Sociotechnika v pojetí informační bezpečnosti znamená přesvědčování a ovlivňování lidí s cílem oklamat je tak, aby uvěřili, že útočník je někdo jiný, a zmanipulovat je k vyzrazení informací nebo provedení určitých úkonů.

Lidé jsou v principu důvěřiví a věří jeden druhému, a proto jsou vůči sociálnímu inženýrství hodně zranitelní. I zdánlivě nevinné informace je třeba chránit, proto by zaměstnanci v organizacích měli dodržovat jednoduché pravidlo: veškeré firemní údaje musí považovat za citlivé a nikomu je nesmí prozrazovat. Mezi nejpoužívanější metody útoku patří Trashing, Phishing, Pharming a Vishing.

Trashing

Trashing je nejstarší technikou a znamená prosévání firemního či bytového odpadu za účelem získání cenných informací. Útočník hledá jakékoli dokumenty spojené s výpisy z účtu, telefonních karet a jiné cennosti. Řada společností i domácností má kontejnery umístěny v nestřeženém okolí svých budov, a tím se stávají snadno dostupné pro útočníka. Tato metoda je velmi účinná, ale u sociotechnika méně oblíbená, protože ne každý má žaludek na prohrabávání popelnic. V poslední době ale útočníkům napomáhá třídění odpadu, prohledávají pouze kontejnery na papír a nemusí se prohrabávat veškerým hnijícím odpadem.

Obranou proti této technice je přejít na elektronickou formu citlivých dokumentů nebo zbavovat se důležitých dokumentů fyzickým zničením, nejlépe zpopelněním. Ani skartace papírových dokumentů není bezpečná, protože pokud si dá někdo tu práci, dokáže rozřezané papíry složit zpět jako puzzle.

Phishing

Phishing nebo-li „rybaření“ je podvodná technika používaná na Internetu k získávání citlivých a užitečných údajů od obětí, jako jsou hesla, čísla kreditních karet, PIN a podobně. Využívá se k tomu rozesílání e-mailových zpráv, které se tváří jako oficiální žádost banky či jiné podobné instituce s odkazem na podvodné stránky, kde vyzývají adresáta k zadání jeho přihlašovacích údajů. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni s jeho účtem libovolně manipulovat.

Obranou před touto technikou je nepovažovat Internet za zdroj pouze důvěryhodných informací, nepoužívat hypertextové odkazy zahrnuté přímo v e-mailu, nikomu nesvěřovat důvěrné informace. Je vhodné používat aktualizovaný antivirový software a prohlížeče či doplňky, které umějí phishing rozpoznat.

Pharming

Pharming označuje činnost, při které útočníci přesměrují internetovou komunikaci z jednoho webu na jiný. Pharming spočívá v modifikaci DNS záznamů změnou záznamů v souboru hosts u jednotlivých počítačů s operačními systémy Windows. Nic netušící uživatel je pak i při zadání správné adresy internetového bankovníctví přesměrován díky změněným DNS záznamům na podvodnou stránku. Jestliže je tato falešná stránka dobře vypracovaná, pak je nízká šance, že by uživatel na podvod přišel.

- Obranou proti tomuto útoku je zajistit ochranu samotného souboru s názvy hostitelů a mít správně nastavený a aktuální antivirový program kontrolující nejen všechny soubory posílané elektronickou poštou, ale také vše, co je spouštěno a stahováno z webu. Další možností je používání nástrojů, které zobrazují doplňující informace o právě zobrazovaných webových stránkách (Netcraft Toolbar).

Vishing

Vishing těží z důvěry v telefonní služby, je to zneužívání VoIP technologie (Voice over Internet Protocol) pro vylákání osobních a finančních informací za účelem osobního obohacení. Vishing napodobuje obvyklý způsob komunikace lidí s jejich finančními institucemi. Oběti jsou dotazovány na čísla účtů, hesla nebo čísla sociálního zabezpečení. Tyto údaje jsou poté prodávány v Internetu a používány k podvodům se získanou identitou. S příchodem VoIP již nemusí být na konci telefonního spojení pevná linka, ale třeba i počítač, který lze snadno pro tyto účely zneužít.

Obrana proti vishingu zůstává pouze na uživateli a vždy, když přijde na identifikační údaje, je vhodné používat zdravý rozum. V případě finančních institucí je vhodné žádat o ověření totožnosti například požádáním, jakou transakci jsme naposledy provedli. Zloděj k takovým informacím nebude mít pravděpodobně přístup.

Základní principy zabezpečení

Zabezpečení IT znamená proces dosažení a udržení důvěrnosti, integrity, dostupnosti, prokazatelnosti odpovědnosti, autenticity a spolehlivosti informací a služeb IT na přímé úrovni. Abychom dosáhli kompletního zabezpečení počítačové infrastruktury, musíme splnit tyto podmínky:

- ***Vrstvená bezpečnost*** - bezpečnost musí být vrstvená. Potřebujeme firewall jako základní bránu pro filtrování mezi bezpečnostními zónami, potřebujeme antivirus a antispam, potřebujeme VPN pro bezpečný přístup zaměstnanců, popř. pro propojení korporace s jejími partnery, a potřebujeme další ochrany v závislosti na službách a jejich důležitosti (šifrování, elektronické podpisy, atd.).
- ***Řízení přístupu*** – musíme určit a nastavit, kdo bude mít povolen přístup do sítě. Jedním z doporučovaných postupů je všechno zablokovat a potom výslovně povolit jen to, co daný uživatel potřebuje ke své práci.

- ***Uvědomění uživatelů*** – školení uživatelů a posílení jejich uvědomělosti v otázkách bezpečnosti je velmi důležité, jen tak pochopí její význam a budou spolupracovat a podporovat zásady zabezpečení.
- ***Monitorování*** – je zapotřebí systémy průběžně monitorovat a ověřovat, jestli jsou stále bezpečné a odolné vůči útokům. Sledování provádíme pomocí detekčních systémů IDS (Intrusion Detection System).
- ***Aktualizace systémů*** – je potřeba sledovat, jestli pro daný systém nejsou k dispozici nějaké aktualizace či záplaty. Mnohé novější operační systémy dokáží automaticky připomínat stahování aktualizací.

Budoucnost bezpečnostních funkcí

Do budoucna lze očekávat, že pokročilé bezpečnostní funkce, které byly doposud dostupné pouze velkým společnostem, se rozšíří také mezi jednotlivce a domácnosti. Aby výrobci těchto bezpečnostních zařízení získali náskok před konkurencí, budou se snažit implementovat další nové funkce, např. podporu mobilních zařízení a kompletní podporu protokolu IPv6, ten je v současnosti podporován u některých výrobců pouze částečně.

Otázky:

- Co znamená v informatice narušení bezpečnosti?
- Jaké druhy útoků znáte?
- Co je zranitelné místo?
- Co je to sociální inženýrství?
- Vysvětlete pojem Trashing.
- Vysvětlete pojem Phishing.
- Vysvětlete pojem Pharming.
- Vysvětlete pojem Vishing
- Jakým způsobem zajistíme bezpečnost počítačové infrastruktury?

- **Použité zdroje:**

NORTHCUTT, Stephen a kol. *Bezpečnost počítačových sítí*. 1. vyd. Brno: Computer Press, 2005. 592 s. ISBN 80-251-0697-7.

THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. 1. vyd. Brno: Computer Press, 2005. 344 s. ISBN 80-251-0417-6.

http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_bezpe%C4%8Dnost, [2.12.2012]

<http://www.sociotechnika.ic.cz/web/web/czech/index.html>, [2.12.2012]