OBSAH

KYBERNETICKÁ BEZPEČNOST A LEGISLATIVA

KYBERNETICKÁ BEZPEČNOST

JAKÁ JE SITUACE?

1. Co nás může ohrozit? Proč? Koho?
2. Řadu věcí jsme si způsobili sami dobrovolně
3. Závislost celé společnosti na IT
4. Závislost velké části ekonomiky na IT
5. Bezpečnost jako klíčový faktor při rozhodování o investicích i zahraničních společností
6. Kyber války
7. Tlak na přechod dalších aktivit do kyber prostoru

KYBERKRIMINALITA

1. Jde o velmi výdělečný byznys (stejně jako drogy, zbraně..)
2. Pravidla normálního podnikání
3. Prodej útoků
4. Skupina, kde se navzájem neznají
5. Útoky do jiné země
6. Minimální šance na odhalení
7. Prodej napadených počítačů
8. Napadené počítače tvoří tzv. botnet, z toho útoky

Botnet je označení pro softwarové agenty nebo pro internetové roboty, kteří fungují autonomně nebo automaticky.

Termín je nejvíce spojován s malware, kdy botnet označuje síť počítačů infikovaných speciálním software, který je centrálně řízen.

Botnet provádí nežádoucí činnost (rozesílání spamu, DDoS útoky a podobně). Představují jednu z největších hrozeb v posledních několika letech, kdy se vzhledem k vývoji škodlivého software a celkové propojenosti daří napadat i stovky počítačů, které pak mohou být ovládnuty na dálku jedním řídícím přístrojem.

Následně je možné ovládat je pomocí tzv. zadních vrátek, instalovat potřebné aplikace bez vědomí uživatele a využívat je k různým účelům.

SOUČASNÁ SITUACE V OBRANĚ PROTI KYBER ÚTOKŮM

1. Velmi špatná
2. Spíše se stále zhoršuje
3. Útočníci jsou v předstihu před ochranou IS
4. Uživatelé si řadu rizik neuvědomují
5. Útoky v oblasti IT jsou v určitých komunitách považovány hrdinské činy, ač se jedná o trestnou činnost.
6. Útočníkům vůbec nedojde, že jejich útok (který považují za zábavu) může způsobit tragédii.

NÁSLEDKY

1. Výpadek IT technologií z důvodů napadení např. při krizových situacích (např. při záchranných pracích, při řešení velké havárie apod.) by mohl být fatální.

2. Výpadek informačního systému všeho druhu
3. Chaos
4. Neschopnost organizovat záchranné práce
5. Výpadky organizací všeho druhu
6. Ohrožení bezpečnosti státu
7. Výpadek IT systémů nemocnic, vodáren, doprava plynu, elektřiny…. přesměrování produktovodů

VYSVĚTLENÍ POJMŮ

DDoS je distribuovaný DoS útok - Distributed Denial of Service attack, charakterizován větším množstvím počítačů, snažících se najednou zahltit cíl útoku.

Útok se nejčastěji využívá k zahlcení webových serverů (např. útok na české zpravodajské servery! v březnu 2013), případně k oslabení nebo vyřazení sítě.

Útok nebývá dlouhodobý, ale bývá konkrétně cílený a často při něm vznikají nemalé ekonomické ztráty.

Cílený DDoS útok může způsobit kolaps určitých systémů.

Často veden bez vědomí majitelů útočících počítačů a jedná se o důsledek napadení a úspěšného infikování těchto systémů.

Infikované systémy můžou být vzdáleně řízeny a jejich služby je si možné zakoupit na černém trhu a směrovat DDoS útok na libovolnou organizaci.

Do těchto útoků se zapojovalo v např. v roce 2013 tisíce českých počítačů a jejich majitelé vědomě či nevědomě riskovali často značné postihy.

Šifrovací funkce E operuje nad M a produkuje C.

$E(M) = C$

V reversním procesu dešifrovací funkce D operuje nad C a produkuje M.

$D(C) = M$

Zásadním bodem šifrování a dešifrování musí být, že získáme původní text, musí platit tato identita :

$D(E(M)) = M$

Kryptografický algoritmus (tzv. cipher) jsou 2 matematické funkce: jednu užíváme pro zašifrování a druhou pro dešifrování

Moderní kryptografie (která je dnes užívána) obvykle užívá tzv. klíč (K).

Když pro šifrování a dešifrování užíváme klíč, pak máme:

$E_K(M) = C \qquad D_K(C) = M$

$D_K(E_K(M)) = M$

Některé typy algoritmů užívají dva odlišné klíče pro šifrování klíč (K_1) a pro dešifrování klíč (K_2):

$E_{K1}(M) = C \qquad D_{K2}(C) = M$

$D_{K2}(E_{K1}(M)) = M$

SYMETRICKÉ ŠIFRY

Symetrická šifra je taková, která pro šifrování i dešifrování používá tentýž klíč. Symetrické (konvenční) šifrování je

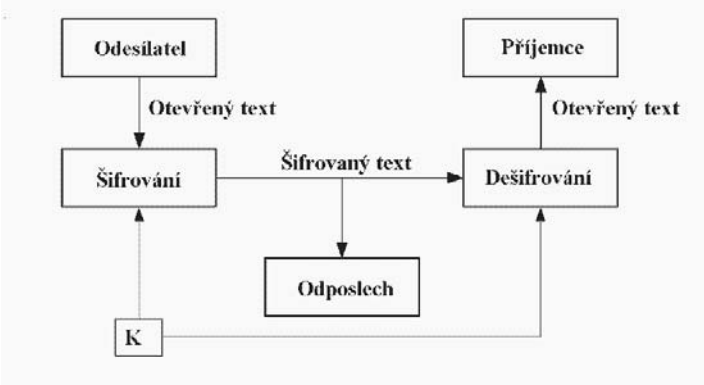
založeno na principu jednoho klíče, kterým lze zprávu (data) jak zašifrovat, tak i dešifrovat.

Výhody:

1. nízká výpočetní náročnost

Nevýhody:

1. příjemce i odesílatel se musí dohodnout na jednom klíči, který budou znát jen oni dva a který je nutno trvale uchovávat v utajení
2. distribuce klíče – jak dostat klíč k příjemci, aniž by se ho chopil někdo nepovolaný
3. nutnost velkého počtu klíčů, protože každé dvě komunikující strany potřebují svůj vlastní tajný klíč a počet klíčů ve velké skupině tak neúměrně narůstá



Obr. 1: Schéma symetrického šifrování.

ASYMETRICKÉ ŠIFRY

Asymetrická šifra používá veřejný klíč pro šifrování a soukromý klíč pro dešifrování. Pokud používáme asymetrickou šifru pro podepisování, pak se naopak

soukromý klíč podpisujícího používá pro podepsání a jeho veřejný klíč pro ověření podpisu.

Asymetrická kryptografie (kryptografie s veřejným klíčem) je skupina kryptografických metod, ve kterých se pro šifrování a dešifrování používají odlišné klíče. (To je základní rozdíl oproti symetrické kryptografii, která používá k šifrování i dešifrování jediný klíč.)

Asymetrická kryptografie je založena na tzv. jednocestných funkcích = operace, které lze snadno provést pouze v jednom směru: ze vstupu lze snadno spočítat výstup, z výstupu však je velmi obtížné nalézt vstup.

Je zřejmé, že šifrovací klíč e a dešifrovací klíč d spolu musí být matematicky svázány, avšak nezbytnou podmínkou pro užitečnost šifry je praktická nemožnost ze znalosti šifrovacího klíče spočítat dešifrovací.

Matematicky tedy asymetrická kryptografie postupuje následujícím způsobem:

Šifrování : $c = f(m, e)$

Dešifrování : $m = g(c, d)$

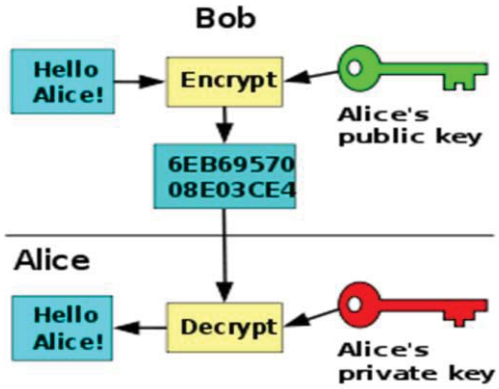
V principu se mohou šifrovací a dešifrovací funkce lišit, zpravidla jsou však matematicky přinejmenším velmi podobné.

Nejběžnějším příkladem je násobení: je velmi snadné vynásobit dvě i velmi velká čísla, avšak rozklad součinu na činitele (tzv. faktorizace) je velmi obtížný. (Na tomto problému je založen algoritmus RSA.)

Klíčem je nazýván řetězec znaků, který je použit při matematické operaci zvané šifrování či dešifrování.

Asymetrické kryptografie využívá tzv. veřejného a soukromého klíče:

1. šifrovací klíč je veřejný, majitel klíče ho uveřejní, a kdokoli jím může šifrovat jemu určené zprávy;
2. dešifrovací klíč je soukromý, majitel jej drží v tajnosti (nejčastěji na čipové kartě, příp. v zašifrované podobě na disku) a pomocí něj může tyto zprávy dešifrovat.



Obr. 2: Schéma asymetrické šifry při šifrování. Zdroj Wikipedie

Kromě možnosti pro utajení komunikace se asymetrická kryptografie používá také pro elektronický podpis, tzn. možnost u dat prokázat jejich autora.

DIGITÁLNÍ PODPIS

Teoretický základ a možnost užití digitálního podpisu byla rozpoznána několik let před jeho praktickou implementací, za první metodu možno považovat RSA schéma (Rivest,

SOCIÁLNÍ SÍTĚ, VÝRAZNÉ NEBEZPEČÍ, KLADY A ZÁPORY

Představují zcela nový druh komunikace mezi lidmi. Dnes často využívány pro sociální inženýrství. Proč? Technické zabezpečení organizací je obvykle již velmi dobré, proto se útočí jinak.

Klady:

1. Umožňují snadno kontaktovat přátele
2. Sdílet s nimi informace například ze zájmových činností, multimédia jako videa, fotky, oblíbené písně a mnoho dalšího
3. Díky nim se můžeme snadno dozvědět konkrétní detaily o dané osobě, najít téma k rozhovoru, poznat nové lidi.

Zápory:

1. Většina pramení právě z jejich otevřenosti prakticky každému návštěvníkovi.
2. Existují výjimky, pomocí kterých se dá předcházet sdílení osobních informací se všemi.
3. Síť Facebook obsahuje poměrně efektivní systém, jak předcházet navštěvování profilu cizími lidmi.
4. Jiné sítě zas vyžadují registraci a zobrazují informace o tom, který uživatel jaký profil navštíví.

PHISHING

Slovo phishing vzniklo z fishing (rybaření) – od roku 2004, česky se někdy překládá jako rhybaření.

Jedná se o podvržený email nějaké velké a známé společnosti, který žádá o ověření totožnosti (např.

elektronická burza eBay, Postbank, Citibank, Paypal). V e-mailu odkaz na stránky, které napodobují stránky známé instituce a požadují informace. Krádež citlivých informací, např. údajů o platební kartě či krádež jména a hesla k nějaké službě, uživatel přijde o peníze.

OBRANA

1. na nic neklikejte!
2. přemýšlejte!
3. posuďte reálnost popisované situace, všímejte si případných odchylek od vzhledu či obsahových prvků, které dopisy od dané instituce obvykle mívají
4. ověřte si dopis u instituce, která jej údajně odeslala (nepoužívejte žádné kontaktní informace uvedené v dopisu, ale obraťte se na kontakt, který pro komunikaci s dotyčnou institucí obvykle používáte a máte ověřen)
5. zadávání jména a hesla pouze na zabezpečené stránky
6. adresu pouze ručně psát

Pokud jste už prozradili citlivé údaje

1. zrušte účet, vytvořte nový, zablokujte kartu apod.
2. hlídejte si průběžně transakce na bankovním kontě, aktivity svých uživatelských účtů v různých službách apod.

PHARMING

Pharming je modernější a nebezpečnější nástupce phishingu. Ke své činnosti využívá překladu jména serveru na

ZDRAVOTNICKÁ INFORMACE Z HLEDISKA BEZPEČNOSTI A HROZEB

DIGITÁLNÍ STOPA

Digitálními stopami jsou myšleny informace, které po sobě uživatel zanechává jak v prostředí internetu, potažmo jako součást souborů.

Tyto informace mohou být potenciálně zneužitelné a často o svém tvůrci prozradí víc, než by sám chtěl.

Často navíc zůstávají viset na internetu roky, bez jakýchkoliv zásad, jak s nimi nakládat například v případě uživatelova opuštění profilu, jeho smrti a dalších okolností.

1. Nevědomá stopa: Metadata o vstupu uživatele na stránky, jaké má fonty, jaký prohlížeč, odkud pochází, co o něm prohlížeč prozrazuje, jaká verze prohlížeče, cookie, na jaké pracuje platformě, tzv. Internetový fingerprint
2. P2P sítě, stahování
3. Vědomá stopa: sociální sítě, seznamky, spolužáci, blogy, chaty
4. Vědomě nevědomá
5. Fotografie + GPS, spojování informací, sběr a korelace dat, cloudy
6. Metadata u wordu
7. Google GPS lokátor, databáze sítí, SSID (identifikátor bezdrátové sítě), mobilní telefony
8. Spojuje se více věcí, často nevíte pozadí

V oblasti zanechávání stop je nutné rozlišovat mezi aktivními a pasivními stopami.

Aktivní stopy vznikají přičiněním uživatele – vytvářením profilů, přispíváním na diskusní fóra, interakcemi na sociálních sítích, nahráváním fotek či jiných souborů a podobně.

Pasivní stopy pak vznikají jako vedlejší produkt uživatelovy aktivity – jsou to různé záznamy serverů o chování konkrétního návštěvníka, délce návštěvy a aktivitě na daném webu, o jeho IP adrese a dalších údajích.

K těmto údajům samotný uživatel obvykle nemá přístup a může je ovlivňovat maximálně svým chováním či některými nastaveními (například prohlížeče, využíváním proxy a podobně).

KOHO CO ZAJÍMÁ:

Marketing sleduje mimo jiné pohyb po uživatele po internetu, aktivitu na různých stránkách, dobu výskytu na stránkách, klikání na odkazy, preference uživatele („to se mi líbí“ na Facebooku) a mnoho dalších aspektů.

Marketingové společnosti obvykle data aktivně zaznamenávají a obchodují s nimi v obrovském množství.

Většina stránek, které se tváří, že jsou zdarma, ve skutečnosti funguje na bázi prodeje či výměny informací o uživatelích, případně data využívají pro personalizaci reklamních sdělení.

Forenzní vyšetřování bere digitální stopu jako důkazní materiál, sleduje podle potřeby množství dat, která pak hrají roli v objasňování trestné činnosti.

Může sledovat pohyb uživatele po síti, dobu přihlášení, soubory nahrané na internet i místní soubory například v