DUM 3 téma: Bezpečnost na internetu (EP4)

ze sady: 3 **tematický okruh sady:** III. Ostatní služby internetu
ze šablony: 8 - Internet **určeno pro:** 4. ročník
vzdělávací obor: 26-41-M/01 Elektrotechnika - Elektronické počítačové systémy
vzdělávací oblast: odborné vzdělávání
metodický list/anotace: viz VY_32_INOVACE_08303ml.pdf

Bezpečnost IT jako pojem

Moderní společnost využívá prostředky ICT masivně ve všech oblastech národního hospodářství i v soukromí. Z těchto důvodů je oblast bezpečnosti těchto prostředků i jejich funkcionalit velmi aktuální.

Z hlediska bezpečnosti rozlišujeme u informačních systému subjekty (tedy to co se snažíme ochránit) bezpečnosti:

- hardware
- software
- data

V praktickém pohledu vycházíme z úvahy o nahraditelnosti jednotlivých komponentů informačního systému a tedy o míře nutnosti je chránit. Hardware i software lze v případě závady či napadení nahradit za předem jasně dané ceny dodavatelů. Zvláštní kapitolou jsou však data v informačním systému – která jsou mnohdy produktem vlastního podnikatelského či pracovního úsilí. Určit jejich cenu není tedy tak snadné jako u předchozích položek a z pohledu informatiky užíváme tzv. cenu obnovovací – zjednodušeně vyjádřitelnou jako náklady na opětovné získání dat v případě jejich ztráty či zničení. Z tohoto náhledu vyplývá i poznatek, že řada dat v informačním systému může mít cenu nevyčíslitelnou.

Ze známé (či rámcově odhadnuté) ceny ochrany-hodných komponent informačního systému pak můžeme metodami řízení rizika určit míru akceptovatelného rizika a tedy i minimální požadovanou úroveň bezpečnosti. Základní poučkou bezpečnosti totiž je, že bezpečnost není stav kterého by bylo možné v konečném čase dosáhnout, ale naopak nikdy nekončící proces, kterým můžeme její míru zvyšovat (či snižovat). Postupnými iteracemi sice klesá pravděpodobnost využití zranitelného místa k realizaci útoku, ovšem náklady na další její zvyšování rostou exponenciálně. Dříve či později tedy každý bezpečnostní mechanismus narazí na své hranice, kdy další zvyšování zabezpečení není ekonomicky opodstatnitelné a systém se soustředí na udržování dosažené úrovně, reakcí na bezpečnostní incidenty a jejich zpětnou analýzu.

Komponenty bezpečnosti

Na úrovni střední školy můžeme samotný pojem bezpečnost rozdělit na

Důvěrnost dat

Důvěrností rozumíme schopnost informačního systému zpřístupnit požadovaná data (či informace – v tomto kontextu je rozdíl nevýznamný) pouze oprávněnému uživateli (lhostejno zda se jedná o lidskou bytost nebo jiný informační systém) a naopak neoprávněnému žadateli přístup odepřít a pokus o narušení bezpečnosti reportovat.

Spolehlivost systému

Obecný termín spolehlivost každý intuitivně chápe, v kontextu počítačové bezpečnosti se jedná o míru uspokojivého vyřešení legitimních požadavků kladených na informační systém, rozložených statisticky normálně v čase. Konkrétněji pak o schopnost systému reagovat na legitimní (uvedené v slovníku nebo use-case diagramech) požadavky a dávat uživateli výstupy v místě, čase a formě dle jeho potřeb.

Do kapitoly spolehlivosti tedy řadíme i měření rychlosti odezvy systému na normalizovaný požadavek, odolnost systému vůči zahlcení (oprávněnými i neoprávněnými požadavky) či měřitelnost dostupnost služeb v průběhu určeného časového intervalu. V profesionálních službách pak hovoříme o úrovni SLA, uváděné v % (např 99,99%) a to v intervalu nejčastěji měsíce. Za nedodržení garantované dostupnosti pak dodavatel (či provozovatel informačního systému) většinou poskytuje smluvně určenou slevu, zcela výjimečné je naopak za nedostupnost platit pokuty (resp. Je fakticky vymáhat).

Důvěryhodnost výstupů systému

Vzhledem ke zmíněné závislosti moderní společnosti na informačních systémech je otázka jejich důvěryhodnosti zcela klíčová. Samozřejmě u služeb orientovaných spíše zábavně (Facebook, MySpace apod.) je důvěra k jejich výstupům věcí osobního rozhodnutí či zájmu, služby provozované státní mocí či klíčovými formami mnohdy musíme za důvěryhodné považovat a jejich výstupy mají tuto důvěryhodnost inherentní či fakticky danou zákonem.

Výstupy informačního systému, kterým z nějakého důvodu důvěřujeme a využíváme je pro další rozhodování či práci pak nazýváme autoritativní.

Bezpečnostní hrozby

Vše, co může způsobit újmu aktivům informačních systémů prostřednictvím využití jeho slabin, či bezpečnostních děr nazýváme hrozbami. Úkolem správy rizik je tedy popsat a zhodnotit pravděpodobnost jejich vzniku a určit hrozby reálné a méně nereálné. Základní rozdělení hrozeb je:

Objektivní

Způsobené vnějšími vlivy, jejichž výskyt můžeme pouze statisticky předpokládat a vliv pouze omezit.

- požár
- povodeň,
- zemětřesení,
- průmyslová havárie, atd …

Subjektivní

Zaviněné člověkem s přímým vztahem k informačnímu systému či datům v něm.

- sabotáž
- zneužití dat,
- zavlečení viru,
- kompromitace hesel či klíčů…

Bezpečnost komunikace

Pojmový aparát

Základními pojmy v této oblasti jsou:

- identifikace – jednostranný úkon, prohlášení uživatele za určitou entitu (z objektového teorému spíše instanci entity)
- autentizace – začasto dvojstranný proces, kterým se identita ověřuje

- autorizace – ad-hoc ověření, že daný uživatel je oprávněn vykonat činnost, kterou od informačního systému požaduje; provádí se opakovaně při každém požadavku

Typy autentizace

Metody ověření identity lze rozdělit do těchto skupin:

Metody založené na znalosti

Základem těchto metod je premisa, že toliko oprávněný uživatel disponuje nějakou znalostí či informací a svou identitu potvrzuje sdělením takové informace. Samozřejmě příslušný informační systém musí být schopen její správnost ověřit.

Z praktického pohledu bývá takovou informací typicky alfanumerické heslo či číselný pin, obecně se ale může jednat i o znalost umístění tajného vypínače, správné syntaxe příkazů, nestandardních čísel portů a podobně.

Metody této skupiny jsou jednoduché implementačně prakticky bez nákladové jak na straně systému tak uživatele ale jejich bezpečnost (zjednodušen pravděpodobnost neoprávněného vstupu) je poměrně nízká. Samotná znalost je totiž jednoduše napodobitelná – ať při spolupráci oprávněného uživatele (např. sdělí heslo 3. osobě) či metodami statistickými či zpravodajskými (uhodnutí heslo, odpozorování pohybů na klávesnici, různé formy násilí atd.). Z pohledu informačního systému pak nelze naprosto rozlišit jednotlivé uživatele, pokud disponují správnými znalostmi.

Nejčastěji užívané metody na bázi hesel pak lze poněkud zlepšit alespoň zavedením minimální délky hesla a rozšířením množiny použitých symbolů (velká písmena, číslice, ne-alfanumerické znaky atd.) či technikou jejich ověřování (pauza po několika špatných pokusech). Samotná otázka střední doby prolomení textového hesla je pak spíše téma z oblasti statistiky.

Metody založené na vlastnictví

Tyto metody využívají předpokladu, že pouze oprávněný uživatel je vlastníkem či držitelem určitého předmětu (autentizačního tokenu), který jejich identitu potvrzuje. Pro občana je takovým předmětem například občanský průkaz, v informačních systémech spíše různé typy karet, čipů či fyzických klíčů. Obecným požadavkem na autentizační tokej je jeho unikátnost, nenapodobitelnost, nemožnost duplikace ale na druhou stranu i přenosnost a rozumná cena

výroby. Některé tyto požadavky jsou v opozici, náklady jsou závislé na počtu autentifikovaných uživatelů kdy kromě jasného počtu čteček či jiných terminálů musí být tokeny vybaveni i jednotliví uživatelé.

Běžný uživatel přichází do styku buď s jednosměrnými magnetickými kartami, či obousměrnými čipy – obojí v tisícovkách různých formátů a vzhledů. Dříve používané magnetické karty pracují pouze jako nosiče jednoduché autentizační informace a de-facto jako náhrada znalosti hesla v předchozí metodě. S vhodnou technikou je tak možné informaci z karty načíst a následně vyrobit dokonalý duplikát – viz nebezpečí skimmingu u bankomatových karet. Karty či obecně tokeny čipové pak realizují dvoustrannou komunikaci s čtečkou formou výzva-odpověď, kdy samotný obsah tokenu není čtečce přístupný (srovnej - objektový přístup a metody zapouzdření) a informační systém porovnává zda na určitou výzvu vrátil token očekávanou odpověď.

Samostatnou podmnožinou jsou metody biometrické, kde je v roli autentizačních tokenů samo lidské tělo, přesněji jeho markanty. Ty splňují prakticky všechny požadavky na takový autentizační předmět a dokonce odpadá nutnost uživatele dodatečně tokeny vybavovat. Zcela bezproblémová je i otázka přenosnosti takových tokenů či možnost jejich ztráty či zapomenutí (např. otisky prstů pravděpodobně čtenář ráno doma nezapomene).

Problematická je však část terminálů-čteček, které sice prošly v posledních letech dramatickým vývojem, přesto jejich spolehlivost neumožňuje zcela samostatné nasazení a při rozsáhlejších provozech pak zvyšuje i náklady na pravidelnou údržbu (čištění atd.). Nelze opomenout ani psychologické aspekty, kdy je dosti obtížné přesvědčit uživatele např. aby pravidelně vkládal hlavu do čtečky a nechal si přístrojem scannovat duhovku oka.

Nejčastějšími metodami je snímání otisků prstů, dlaní, struktury duhovky oka, charakter hlasu, styl chůze, tvar obličeje a podobně.

Metody kombinované

Jak název napovídá, kombinují předchozí přístupy vlastnictví a znalosti. Tím lze efektivně využít jejich dobré vlastnosti a potlačit negativní.

Nejčastější a čtenáři jistě známou kombinací je vlastnictví karty (magnetické či čipové) a znalost PINu. Funkční je pak až kombinace obojího a případná ztráta či duplikace karty ještě nezpůsobí okamžité narušení (kompromitaci) bezpečnosti. Obdobně přečtení či sdělení PINu bez

předání karty také bezpečnost zcela nenaruší. Možná je i kombinace biometrického tokenu hesla či PINu.

Bezpečnost přenosu dat

V prostředí rozsáhlých sítí většinou řešíme úlohu jak přenést informace od jednoho uzlu k druhému, s využitím prostředí (komunikačních linek) nad kterými nemáme plnou kontrolu (mnohdy spíše nemáme kontrolu vůbec žádnou). Pro realizaci takové úlohy je nutné nejprve rozhodnout, zda přenášené informace jsou vůbec důvěrné a ochranu požadují – či jakou míru rizika přijmeme (viz výše). Může i nastat situace kdy není nutno chránit obsah přenášených dat, ale kupříkladu identifikaci jejich zdroje či data odeslání a podobně.

Základní metody ochrany přenášených dat proti útokům na důvěrnost (obsah dat), integritu (shoda obsahu s verzí odeslanou) a autenticitu (potvrzení skutečného autora) zahrnují:

Steganografii

Kdy Před útočníkem skrýváme samotný fakt, že je zpráva přenášena. Buď použitím neobvyklého komunikačního kanálu v kombinaci s přenosem neškodné zprávy prostřednictvím kanálu, který útočník sleduje; či skrytím zprávy do jiné, navenek neškodné. Takovou „jinou“ zprávou může být v digitálním věku třeba bitmapový obrázek-fotografie kde je domluveným způsobem upraven např. každý n-tý bit tak aby byl nosičem tajné zprávy. Navenek se tato změna viditelně v obrázku neprojeví (typicky u 16-bit bitmapy dojde ke změně jasnosti některého bodu o 65tisícinu, což je zcela nepostřehnutelné) a pouze správný příjemce, který ví co má hledat, tajnou zprávu znovu složí. Zvláštní variantou jsou pak neviditelné vodoznaky, které autoři umisťují do fotografií, aby mohli v budoucnu zpětně prokázat své autorství v případě sporů. Tato metoda je zvláště u fotografií na internetu stále populárnější a kvalitně provedený vodoznak nelze zcela odstranit ani překomprimováním či deformací obrázku.

a

Kryptografii

Což je rozsáhlá skupina metod, kterým převádíme zprávy z čitelné („otevřené“) podobny do formátu útočníkem nevyužitelné. Zpráva je tak sice přenášena viditelně a případný útočník ji může zachytit, spoléháme však na zvolenou kryptografickou metodu že útočník nebude schopen otevřenou formu zprávy rekonstruovat.

Pro účely této publikace můžeme kryptografické metody souhrnně označit jako šifrování (což je značným zjednodušením), kdy šifru chápeme jako algoritmus převodu zprávy do uzavřené podoby a k němu inverzní (ve smyslu funkčnosti, nikoliv matematickém!) pak algoritmy dešifrovací. Zvláštními metodami jsou kryptoanalytické, které se naopak snaží získat otevřenou verzi zprávy bez znalosti dešifrovacího algoritmu a/nebo některé z nutných náležitostí jeho regulérního použití.

Šifrovacích algoritmů existuje celá řada a jejich kompletní přehled je mimo rozsah této publikace. Lze obecně rozlišit šifry substituční (kdy jsou symboly vzájemně zaměňovány dohodnutým způsobem), proudové (kdy je otevřená forma zprávy zpracovávána postupně symbol za symbolem) a blokové (kdy jsou zpracovávány části zprávy pevné či proměnné velikosti samostatně).

My však rozdělíme šifrovací metody toliko do dvou skupin: symetrické a asymetrické metody.

Symetrické metody

Nosnou myšlenkou všech těchto metod je společný šifrovací klíč (např. „heslo“ ale může jím být i jakákoliv posloupnost bitů a podobně) pro obě komunikující strany resp. Pro každý komunikující pár. Šifrovací a dešifrovací algoritmy jsou pak skutečně inverzními funkcemi a problém přenosu zprávy nedůvěryhodným prostředím se zjednodušuje na přenos šifrovacího klíče. Ten lze mezi komunikanty vyměnit před započetím komunikace nebo jiným komunikačním kanálem (který například kapacitně nedostačuje pro přenos všech zpráv, ale považujeme ho za bezpečný). Slabinou této metody je nutnost velkého množství klíčů s rostoucím počtem komunikujících dvojic nebo růst pravděpodobnosti jeho kompromitace, pokud by jej sdílelo více komunikantů zároveň. Typickou symetrickou šifrovací metodou jsou AES či DES.

Asymetrické metody

Využívají klíče vázané na konkrétního komunikanta, který disponuje párovou dvojicí klíčů, označovaných jako „veřejný“ a „soukromý“. Základem bezpečnosti je elementární matematika kdy (extrémně zjednodušeně) po vynásobení dvou dostatečně velkých prvočísel nelze ani při znalosti výsledku jednoznačně určit která čísla původně do výpočtu vstoupila. Hovoříme tedy o bezpečnosti implicitní, kdy je naopak znalost šifrovacího algoritmu (například

RSA) zcela volná a útočníkovi nikterak kryptoanalýzu nezjednoduší. Další výhodou je snížení počtu klíčů, kdy každý komunikant potřebuje pouze klíče dva, bez ohledu na počet protistran se kterými si zprávy vyměňuje. Pro účastníka je základní podmínkou udržovat v tajnosti svůj soukromý klíč – ze kterého je možné veřejný zpětně odvodit. Opačný postup není z principu analyticky možný.

U asymetrických algoritmů je možné šifrování buď cílené – pro určitého příjemce, či podepisování – konkrétním zdrojem. V prvním případě použije odesílatel znalost veřejného klíče příjemce a zprávu převede do uzavřeného formátu, který již nedokáže zpětně rekonstruovat ani on. Pouze držitel soukromého klíče může provést převod zpět na otevřenou formu.

Druhá varianta se nazývá digitální (či konkrétněji elektronický) podpis. Tato metoda chrání především integritu a autenticitu zprávy, nikoliv její důvěrnost. Odesilatel ze zprávy spočítá pomocí hash funkce (funkce, která ze zprávy libovolné délky vytvoří řetězec pevné délky – přičemž dvě velmi podobné zprávy mají hash velmi odlišný, např. CRC, MD5 a podobně) její otisk, který následně zašifruje svým soukromým klíčem. Nedůvěryhodným prostředím pak předává zprávu samotnou (v otevřeném formátu), vytvořený podpis a případně svůj veřejný klíč (pokud ho příjemce již nemá, viz dále). Příjemce ze získané zprávy také spočítá otisk, pomocí veřejného klíče odesilatele dešifruje podpis a získaný otisk porovná s tím, který spočítal sám. V případně shody považuje zprávu za integritní (během přenosu ji nikdo nezměnil) a autentickou (odeslal ji skutečně ten, kdo to o sobě tvrdí).

Uvedený postup je založen na principiální bezpečnosti a jeho všeobecná znalost tak není na újmu jeho bezpečnosti. Zůstávají pouze dvě místa, kde může selhat – možnost kompromitace soukromého klíče odesilatele a podvržení veřejného klíče útočníka místo veřejného klíče původního odesilatele zprávy.

První riziko musí nést každý účastník sám a klíč například ukládat pouze na přenosná média, nebo rovnou do čipové karty a podobně. Druhý možný problém lze omezit vytvoření systému důvěryhodných identit a podepisováním samotných veřejných klíčů. Hovoříme pak o „certifikátech“.

Principiálně stačí najít důvěryhodnou autoritu (osobu či častěji organizaci), která shromažďuje veřejné klíče účastníků a na žádost je předává dalším. Mnohdy tato organizace sama klíče vytváří a hovoříme pak o certifikační autoritě. Její důvěryhodnost je pak v systému dogmatická a to buď díky jejímu dobrému jménu, nebo povinně ze zákona (kvalifikované

certifikáty). Tato certifikační autorita většinou i veřejné certifikáty účastníků podepisuje svým soukromým klíčem a lze tak ověřit, že certifikát (a tedy veřejný klíč) patří skutečně dané osobně a nikoliv útočníkovi. Potřebné je pouze zajistit bezespornou distribuci veřejného klíče samotné certifikační autority. Ty bývají součástí přímo instalace operačního systému, případně je možné si jej vyzvednou osobně na kontaktním místě či provozovně.

Certifikační autorita pak jako svůj zcela nejdražší majetek chrání právě svůj soukromý klíč, při jehož kompromitaci by se celý systém rozpadl. Bohužel jinak dokonalý systém sabotují sami uživatelé, kteří na upozornění o podezřelém veřejném certifikátu (typicky u www stránek), který nebyl podepsán důvěryhodnou autoritou nebo trpí jinou vadou, reagují automaticky schválením výjimky bez další analýzy.

Zdroje:

- Archiv autora