Attack Tree Modelling

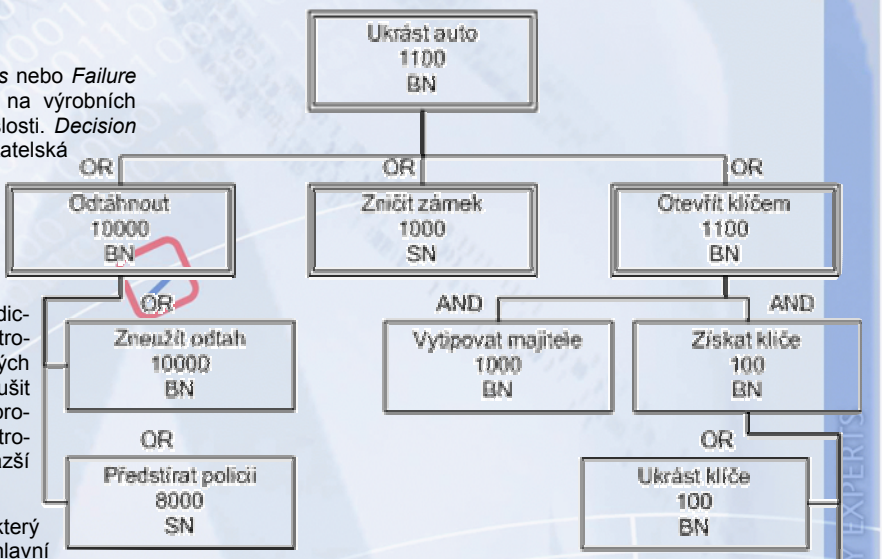
Obecné použití ATM

Jedním z nezbytných kroků při zavádění nebo podpoře systému řízení bezpečnosti informací (ISMS – Information Security Management System) je provedení analýzy rizik informačního systému. Je nutné, abychom znali hodnotu našich aktiv zejména dat a hrozby a slabiny našeho systému včetně jejich úrovně. Podle výsledné míry rizika pak teprve můžeme zavádět bezpečnostní protiopatření v podobě nových technologií.

Pro analýzu rizik informačních systémů se dnes se prakticky používají dva druhy metodik – kvantitativní a kvalitativní. V prvním případě stanovujeme riziko jako předpokládanou finanční ztrátu v určitém časovém období (ALE – Annual Loss Expectancy). Při hodnocení rizik kvalitativní metodikou používáme různé škály pro hodnocení aktiv nebo hrozeb a zranitelností. ATM můžeme považovat za kvantitativní metodiku pro analýzu rizik IS. Nejedná se však o metodiku, s kterou můžeme provést plnohodnotnou analýzu rizik jako proces při zavádění nebo podpoře ISMS. ATM může jako doplněk jiné metodiky pomoci při zjišťování největších slabin různých systémů a nalézání řešení, jak minimalizovat negativní dopady na aktiva organizace.

Obecné použití Attack Tree Modelling

V průmyslu se již dlouho používají tzv. *Fault Trees* nebo *Failure Trees*, pomocí kterých se zjišťují možné chyby na výrobních linkách, co mohou způsobit, jejich vazby a souvislosti. *Decision Trees* pomáhají identifikovat a hodnotit podnikatelská rizika. Bruce Schneier (významný odborník na kryptografii) aplikoval v roce 1999 známé a vyzkoušené postupy na metodiku pro analýzu rizik informačních systémů a nazval ji *Attack Tree Modelling*.



Použitím stromu útoku můžeme formálně, metodickým způsobem identifikovat a ohodnotit rizika. Stromová struktura je grafickým znázorněním různých hrozeb nebo způsobů útoků, které mohou narušit informační systém a tím způsobit nedostupnost, prozrazení nebo narušení integrity dat. Po vytvoření stromové struktury můžeme najít nejlevnější, nejsnazší nebo nejrychlejší útok.

Prakticky pracujeme tak, že definujeme cíl útoku, který je ve stromu na prvním místě zcela nahoře jako hlavní uzel a různé způsoby dosažení tohoto cíle (narušení systému) tvoří dílčí větve tvořené podřízenými dílčími uzly. Na obrázku je příklad velmi jednoduchého stromu útoku pro ukradení auta. Útočník, v našem případě spíše zloděj, může auto nechat odtáhnout, zničit zámek nebo otevřít auto správným klíčem. Aby auto odtáhl, musí buď zneužít odtah (např. bude předstírat majitele porouchaného vozidla) nebo se převlékne za policistu a nechá auto odtáhnout pro špatné parkování. Pokud bude chtít získat klíče, musí je ukrást nebo najít nebo se domluvit s majitelem. Každý uzel se takto stává jakýmsi subcílem a uzly jemu podřízené popisují způsob, cestu pro jeho dosažení. Uvedený příklad je neúplný a zcela jistě byste ho doplnili o další cesty vedoucí k ukradení auta.

Jednotlivé uzly na stejné úrovni mají mezi sebou přesně daný vztah. Dva uzly si mohou být navzájem alternativou např. tři různé cesty ke zcizení auta. Ale uzly mohou také tvořit dva různé kroky k dosažení cíle. Například, aby mohl zloděj otevřít auto pravým klíčem, musí nejdříve najít majitele a pak od něj ty správné klíče získat. Je tedy pro zloděje velmi obtížné, získat klíče, pokud nezná majitele. Zde pomíjíme možnost, že by si zloděj udělal kopii klíčů třeba v servisu při opravě vozidla. Pro definici vazeb mezi uzly používáme logické operátory AND a OR. Viz obrázek.

Když máme vytvořený strom, můžeme ho doplnit o další informace, které nám pomohou zjistit, jak velké je riziko, že bude auto ukradeno. Jednou z možností, jak ohodnotit všechny způsoby vedoucí k ukradení auta je, přiřadit jim cenu, kterou tyto útoky mohou stát. Pokud bude chtít zloděj odtáhnout auto, musí vlastnit odtahovou službu nebo si ji zaplatit. Stejně tak bude muset vynaložit čas (a čas jsou peníze) k vytipování majitele. Cena je uvedena na obrázku ve druhém řádku každého uzlu. Pokud tedy oceníme všechny uzly, zjistíme, že nejlevnější je vylomit zámek a odjet. Ale proč tato možnost „nevyhrála“? Přidali jsme totiž do hodnocení další parametr a tím je nutnost speciálního nářadí nebo výbavy. Pokud bude chtít zloděj předstírat přísného policistu musí mít uniformu, odznak atd. Zato k ukradení klíčů z majitelovy kapsy stačí zloději pouze zručnost a rychlost.

Pokud tedy budeme hledat nejlevnější způsob ukradení auta, je to zcela jistě zničení zámku. Ale pokud prioritou zloděje bude jednoduchost a až poté cena, nejdříve si vytipuje majitele a poté mu klíče ukradne.

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

Attack Tree Modelling

Použití ATM při analýze rizik informačních systémů

Attack Tree Modelling je určen na poměrně jednoduché a rychlé provádění analýzy rizik dílčích částí systémů se zaměřením na hrozby a zranitelnosti. Součástí tohoto procesu není přímé ohodnocení aktiv zejména datových, které je základním parametrem pro stanovení míry rizika v jiných metodikách analýzy rizik. Určitým způsobem lze toto hodnocení nahradit stanovením maximální ceny, kterou se vyplatí investovat do provedení útoku. Při takovém způsobu ohodnocení nemůžeme s požadovanou přesností říci, jako hodnotu pro nás aktiva opravdu mají. Například v metodice CRAMM se používají tzv. vodítka hodnocení, která přesně zkoumají možné následky při nedostupnosti, prozrazení nebo modifikaci dat a určují jejich hodnotu ve škále. U kvantitativních metodik nebo softwarových nástrojů jako například RiskWatch používáme finanční ztrátu pro hodnocení dopadu na aktiva. Takové hodnocení u ATM bohužel chybí.

Pomocí stromu útoku lze hlavně určit způsoby nebo cesty, které mohou vést k nedostupnosti, prozrazení nebo modifikaci dat. Zjistíme hlavně, jak mohou potenciální útočníci, ať už hackeři nebo zaměstnanci, narušit celý systém a tím zmíněné negativní dopady způsobit. Můžeme najít všechny způsoby, jak nám mohou napadnout webový server hackeři nebo zjistit, zda je pro nás větší hrozbou zaměstnanec s oprávněným přístupem k systému nebo podplacená uklízečka. Výsledky analýzy provedené podle ATM mohou podpořit rozhodnutí pro výběr určitého protiopatření. Attack Tree Modelling může být však pouze skvělým doplněním hodnocení hrozeb a zranitelností při provádění detailní analýzy rizik informačního systému kvalitativní metodikou, tak jak ukazuje uvedené schéma procesu analýzy rizik informačních systémů.

Pozice ATM v procesu analýzy rizik

Fáze 1
Identifikace aktiv
Hodnocení aktiv
Hodnocení dopadů

Fáze 2
Určení působnosti hrozeb
Identifikace slabin
Hodnocení rizika

Attack Tree Modelling
Určení hrozeb, slabin, útočníků
Sestavení stromové struktury
Ohodnocení uzlů

Fáze 3
Určení protiopatření
Návrh implementace

Ohodnocení uzlů

V různých reálných stromech útoku mají jednotlivé uzly několik různých hodnot, které vyplývají z konkrétní situace. Pro ohodnocení můžeme použít jak podrobnou škálu (přesná cena, škála 1-10) nebo pouze hodnoty typu boolean (levné/drahé, složité/jednoduché). Různé hodnoty uzlů mohou být kombinovány, abychom zjistili co nejobjektivněji a nejpodrobněji, jak je systém zranitelný. Můžete najít nejlevnější útok s nejnižším rizikem chycení pachatele, nejjednodušší útok z pohledu zručnosti, nejlevnější útok z nejvyšší pravděpodobností úspěchu atd. Pokaždé, když doplníte strom útoku o určitou charakteristiku útoku, můžete se dozvědět více o bezpečnosti daného systému.

Nejčastěji používané hodnoty

- Pravděpodobnost úspěchu
- Pravděpodobnost chycení pachatele
- Znalost nutná k provedení útoku
- Cena útoku
- Vybavení nutné k provedení útoku
- Úroveň schopnosti útočníka

Jako většina metodik i ATM má svou softwarovou podporu. Kanadská společnost Amenaza vytvořila nástroj SecurITree, jehož součástí jsou i knihovny stromů útoku pro různé systémy (Windows, Oracle, Solaris…). Tyto knihovny mohou pomoci při vytváření stromu, ale obecně může být složité najít všechny způsoby a cesty, kterými lze narušit systém. Velmi záleží na volbě nejvyššího cíle, ke kterému hledáme jednotlivé větve. Pokud to bude „neoprávněné prozrazení informací“, můžeme strom sestavovat i několik týdnů. ATM včetně své softwarové podpory je vhodný zejména pro analýzu dílčích částí informačního systému (jednotlivých služeb, procesů, technologií), nikoli jako komplexní metodika pro provedení detailní analýzy rizik.

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz

Attack Tree Modelling

6 kroků k ohodnocení rizik pomocí metodiky ATM

1. Stanovit rozsah analýzy

Stanovení hranic pro jakoukoli analýzu je velice složité. Analýza může v sobě zahrnovat zkoumání různých oblastí. Budeme analyzovat jednu aplikaci nebo celý systém? Zaměříme se pouze na fyzickou bezpečnost nebo budeme zkoumat i personální a administrativní? Je naším cílem zabezpečit jadernou elektrárnu proti výbuchu nebo přežití celého lidstva? Při definování rozsahu analýzy musíme brát v úvahu také všechny zdroje, které máme k dispozici.

Obvykle chce management nejdříve analyzovat pouze jednu část systému, jednu aplikaci a podle výsledků se rozhodne, jak pokračovat dále. Ale díky propojení různých systémů je velice složité identifikovat a hlavně ohodnotit hrozby lokálně se zaměřením pouze na jednu oblast. Může způsobit výpadek linky na pobočku nedostupnost dat v centrále? Asi ne. Ale co když lidé z centrály potřebovat data, která se ještě nestihla z pobočky replikovat?

Optimální je vždy začít tzv. přehledovou analýzou, při které zjistíme jaké hrozby mohou na jakou část systému působit a jaké dopady mohou nastat. Poté bychom měli určit, do jaké hloubky při analýze půjdeme. Po stanovení míry detailu můžeme přejít k druhému kroku.

2. Identifikovat hrozby a zranitelnosti

Hrozby a zranitelnosti nemůžeme přesně určit bez znalosti analyzovaného systému. Obecné seznamy hrozeb a slabin různých systémů najdeme na internetu, ale nejvíce o hrozbách vždy vědí správci systému nebo uživatelé. V tomto kroku také musíme vzít v úvahu všechny potenciální útočníky, kteří mají zájem narušit bezpečnost daného systému.

Při identifikaci hrozeb a zranitelností systémů bereme v úvahu technické závady nebo selhání technického vybavení, fyzické, logické nebo přírodní hrozby, infiltraci do komunikací apod.

Do kategorie útočníků mohou spadat zaměstnanci, kteří mohou systém poškodit úmyslně nebo jen nevědomky vlastní chybou. Dále je zde konkurence, novináři, různé zájmové (politické) skupiny, hackeři. Ohrozit systém také mohou třetí osoby - smluvní poskytovatelé služeb.

3. Vytvořit strom k narušení systému

Pokud víme, kdo nebo co může poškodit systém, tak je již malý krok k tomu, určit jakým způsobem a co se může stát.

Začneme stanovením základního síle, kterým může být narušení bezpečnosti dat. Ta je narušena, pokud jsou data prozrazena, modifikována nebo nedostupná. Data jsou nedostupná, pokud nefunguje server, je poškozená síťová kabeláž nebo jsou změněna přístupová práva.

Prozradit data může zaměstnanec, mohou být hackrem odposlechnuta na síti nebo je získá pracovník firmy, která upravuje moduly informačního systému.

Postupně začleňujeme všechny hrozby a způsoby potenciálních útočníků do stromové struktury a definujeme vazby OR a AND mezi jednotlivými uzly ve stejné větvi a na stejné úrovni. Stále se musíme držet předem stanovené úrovně detailu.

4. Stanovit parametry hodnocení

Před samotným ohodnocením všech uzlů ve stromové struktuře je nutné specifikovat parametry, které budeme zkoumat a podle kterých budeme hodnotit. Výběr těchto parametrů je závislý na cíli nebo účelu analýzy.

Velice užívaným parametrem je cena útoku, kterou musí útočník zaplatit. Zde se nejedná pouze o peníze, ale také o čas popřípadě další zdroje, které by na finance daly přepočítat. Dále se může hodnotit obtížnost útoku nebo také schopnosti útočníka.

U fyzických hrozeb jako je například povodeň nebo požár nelze mluvit o ceně útoku nebo náročnosti na provedení. Matka příroda se asi nebude moc zajímat o to, na kolik ji přijde povodeň nebo stržení laviny. Můžeme ale ohodnotit pravděpodobnost výskytu, kterou lze zjistit ze statistik nebo historických záznamů.

Na výběru správných parametrů závisí výsledek celé analýzy. Je nutné také vzít v úvahu, jakým způsobem budeme parametry hodnotit a zejména, jestli bude možné stanovit hodnotu u každého parametru.

5. Ohodnotit hrozby (parametry uzlů)

Ohodnocení uzlů není možné provádět bez dostatečné znalosti útoků, útočníků, hrozeb i bezpečnosti obecně. U stanovení ceny za útok většinou nebývá problém, ale přesně odhadnout charakteristiku útočníka je velice složité. Různé typy útočníků mají různé zkušenosti, jsou různě technicky zdatní. Útočníci mohou mít k dispozici jinou výši financí, různý přístup k speciálním prostředkům apod. V případě organizovaném útoku, musíme brát v úvahu, že útočníci budou mít dostatek finančních prostředků a budou ochotni riskovat pobyt ve vězení. Teroristický útok mohou provést lidé, kteří hodlají obětovat i život pro dosažení úspěchu, zde vůbec nelze hovořit o riskování zatčení. Specifickým typem útočníků na informační systém mohou být také studenti, kteří se snaží nabourat systém školy pouze pro zábavu. V tomto případě není nutné brát v úvahu úplatkářství apod.

Ohodnocení fyzických hrozeb je většinou jednodušší. Cenu stanovíme jako velmi vysokou, protože vyvolat přírodní katastrofu se za pár tisíc nikomu nepodaří, pouze matce přírodě. Zde se musíme zaměřit na takové hodnoty typu: pravděpodobnost výskytu, odhad způsobených škod nebo doba trvání. Od charakteristiky potenciálního útočníka nebo hrozby můžeme odvodit, který typ útoku (narušení systému) bude nejvíce pravděpodobný, který typ bude nejúspěšnější.

Hodnoty určujeme pouze u nejnižších (posledních) uzlů. Ostatní výše posazené uzly získají hodnoty přenesením z podřízených. Pokud je vazba mezi podřízenými uzly AND, výchozí hodnota pro uzel nadřízený je zpravidla suma hodnot. V případě vazby OR může být výchozí nejmenší nebo naopak největší hodnota. Není nutné se omezit pouze na tyto dva typy výpočtů, ale můžeme použít jiné například statistické funkce.

6. Zjednodušit strom na reálné hrozby

Správně vytvořený strom útoku na informační systém postihuje všechny možné alternativy narušení. Není však podmínkou detailně zkoumat všechny cesty. Pokud budeme zkoumat strom pro vykradení trezoru, v kterém bude 100 tisíc, můžeme eliminovat všechny cesty, které mají cenu přesahující sumu v trezoru. Pokud budeme zkoumat bezpečnost veřejně přístupného webového serveru, asi nebude na škodu, pokud se informace zde uvedené „prozradí do světa“.

Z poměrně složitého stromu se tak může stát vcelku jednoduchá záležitost. Neměli bychom však seškrtané větve zcela zapomenout, protože může nastat situace, kdy se změní podmínky v systému a například výše zmíněné prozrazení informací se stane tím největším problémem.

Risk Analysis Consultants, Španělská 2, 120 00 Praha 2, Czech Republic, tel.+420 221 628 400, fax +420 221 628 401, rac@rac.cz, www.rac.cz