BEZPEČNOST WWW APLIKACÍ VE SVĚTLE PRAKTICKÝCH POZNATKŮ

Autoři článku: **Karel Miko, Martin Zajíček – DCIT, s.r.o.**
http://www.dcit.cz

Prezentováno na konferenci **Bezpečnosť informácií vo finančnom sektore 2002**
http://www.nmc.sk/bezpecnost2002

Úvod

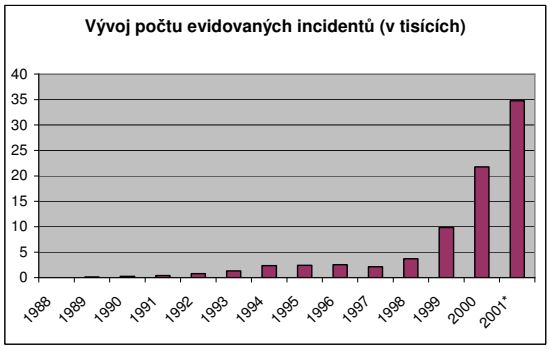
WWW rozhraní je poměrně oblíbená forma elektronického styku mezi podnikem a jeho zákazníky příp. partnery. V oblasti elektronického bankovnictví je jen otázkou času, kdy přímé internetové bankovnictví s přístupem přes WWW bude věc, která se očekává jako „samozřejmost“. Jak je to ale s bezpečností WWW serverů a provozovaných aplikací v reálné praxi? Tento příspěvek se zabývá bezpečnostní WWW aplikací z hlediska praktických zkušeností, které autor jako nezávislý konzultant posbíral z řady penetračních testů a bezpečnostních auditů WWW aplikací.

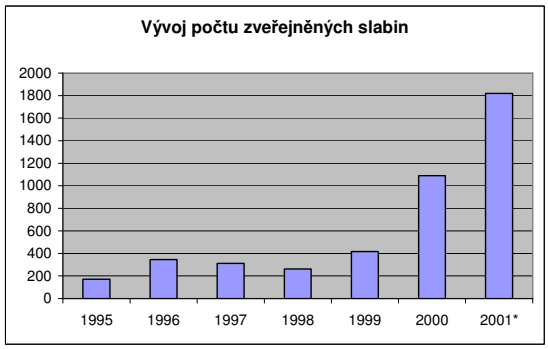
V první části se autor věnuje několika „obecně oblíbeným omylům“ souvisejícím s bezpečností WWW aplikací, v druhé části příspěvku autor diskutuje možnosti, jak uvedeným problémům v praxi čelit, jak jsou která opatření účinná a efektivní, a to nejen z pohledu formální (teoretické) bezpečnosti, ale rovněž z druhé strany tj. z pohledu útočníka.

Ambicí příspěvku rozhodně není poskytnout zaručený návod, jak vybudovat absolutně bezpečnou WWW aplikaci, ani poskytnout kompletní výčet hrozeb souvisejících s provozem WWW aplikací. Cílem příspěvku je podělit se s posluchači o některé autorovy poznatky a zkušenosti z praxe, které pro ně mohou být přínosem v jejich prostřední, při řešení podobných problémů.

Bezpečnost – současná situace

Jako výchozí rámec příspěvku jsem si dovolil citovat trochu statistiky ze zdrojů nezávislé organizace CERT, jedná se o vývoj počtu evidovaných bezpečnostních incidentů (nejedná se pouze o WWW servery) a vývoj počtu zveřejněných bezpečnostních slabin (slabiny v operačních systémech, různých serverových aplikacích apod.).





zdroj: www.cert.org (2001 pouze Q1-Q3)*

I letmý pohled na výše uvedené grafy nám jednoznačně ukazuje nepříliš příznivý trend ve sledovaných oblastech, v obou případech se jedná rozhodně o více než lineární nárůst. Jinými slovy z hlediska bezpečnostních incidentů není momentální situace příliš dobrá, bohužel (nej)horší časy jsou pravděpodobně stále ještě před námi.

Kromě výrazného zvýšení počtu slabin a incidentů zaznamenaly s postupem času podstatné změny rovněž metody používané k útokům. Tyto metody jsou čím dál sofistikovanější a velmi úspěšně drží krok s nejnovějšími bezpečnostními technologiemi (nebo možná spíše naopak), proti některým typům již poměrně dlouho známých útoků nebyly dodnes nalezeny účinné obranné mechanizmy (jako např. DDoS diskutované v další části textu). Neútočí ovšem jenom hackeři či crackeři (rozdíl mezi těmito pojmy zde nechci rozvádět) , ale v poslední době jsou velmi „populární“ útočící automaty (červi apod.), výrazně se tím mimo jiné zkracuje čas mezi zveřejněním slabiny a okamžikem, kdy se tuto slabinu někdo pokusí na Váš systém zneužít.

Budoucnost lze těžko předvídat, ovšem v oblasti bezpečnosti informací a informačních systémů velmi pravděpodobně můžeme očekávat velmi dynamický vývoj, otázkou pouze zůstává, jakým směrem?

Oblíbené omyly o bezpečnosti WWW aplikací (a nejen těch)

1. Šifrovaný přístup = jistota bezpečí

Zabezpečený přístup k WWW aplikacím (tj. použití protokolu HTTP over SSL) lze samozřejmě jen doporučit, neboť je to poměrně spolehlivá cesta znemožnění odposlechu komunikace. Nutno si však uvědomit, že hacker zcela jistě nebude útočit na samotný šifrovací algoritmus, o kterém dobře ví, jak hodně je odolný a kolik desítek či stovek let by potřeboval k rozluštění použité šifry.

V těchto případech je pro útočníka daleko nejjednodušší vytvořit si svůj šifrovaný kanál, což lze v případě protokolu HTTPS výrazně znesnadnit použitím tzv. klientských SSL certifikátů, nicméně z vlastní zkušenosti vím, že v řadě případů je použito běžné HTTPS spojení, které může se serverem navázat prakticky kdokoli.

Úspěšný útok na WWW server v případě použití šifrovaného přístupu protokolem HTTPS může mít naprosto stejný průběh jako v případě nešifrovaného protokolu HTTP. Navíc za jistých okolností může být takový útok „schovaný“ do šifrovaného kanálu obtížněji zachytitelný některými monitorovacími systémy (viz dále).

2. Přeceňování schopností firewallů

Přestože firewall je zcela nepochybně jedna z klíčových komponent zajišťující bezpečnost serverů či jiných zařízení přístupných z Internetu, bývá jeho význam resp. jeho možnosti často přeceňovány. Kvalitně nakonfigurovaný firewall nepochybně zabráním přímým útokům do vnitřní sítě, stejně tak je schopen dobře odfiltrovat přístup k serverům, které chrání.

V případě reálného útoku nebude cílem pravděpodobně přímo samotný firewall, neboť je-li opravdu dobře navržen, je pro útočníka „příliš tvrdý oříšek“ – v ideálním případě není na firewallu z Internetu přístupna žádná síťová služba a solidní firewally jsou velmi dobře odolné vůči známým trikům na „obejití“ filtrovacích mechanizmů.

Útoky jsou obvykle vedeny přímo na konkrétní WWW server, přičemž využívají standardního komunikačního kanálu – tj. TCP spojení na port 80 (http) nebo 443 (https) (tváří se tedy jako uživatel přistupující internetovým prohlížečem), těmto přístupům firewall pochopitelně nebrání. Často se lze také setkat s tzv. útoky přes „prostředníka“, kdy není útok veden přímo na cílový WWW server, ale nejprve na jiný počítač (např. DNS server nebo poštovní server) nacházející se ve stejné demilitarizované zóně jako WWW server, z tohoto počítače je až následně napaden WWW server (což může být výrazně

jednodušší, neboť mezi primárně napadeným počítačem a WWW serverem není obvykle žádná další překážka).

V případě šifrovaných přenosů navíc paradoxně klesá účinnost detekčních nástrojů, které jsou schopny přímo na firewallu odhalit některé pokusy o průnik, konkrétně mám na mysli IDS (Intrusion Detection System) fungující na principu vyhledávání „škodlivých vzorků“ přímo v komunikačních kanálech. Tyto metody mohou v případě WWW serverů velmi dobře fungovat s protokolem HTTP nikoli však s protokolem HTTPS. V této oblasti samozřejmě existují řešení, která pamatují i na HTTPS variantu – šifrované spojení může uživatel navázat nikoli přímo s WWW serverem, ale s firewallem, který se stane „prostředníkem“ v komunikaci, řešením může také být nasazení patřičného detekčního systému přímo na WWW server.

3. Iluze o bezpečnosti WWW serverů (a nejen těch)

Jelikož každý WWW server je „pouze“ software (a nutno zdůraznit, že v řadě případů poměrně dost rozsáhlý), lze očekávat, že přes veškerou snahu výrobce bude obsahovat řadu chyb, z nichž některé mohou mít poměrně významný dopad na jeho bezpečnost.

O pravdivosti předchozího tvrzení nás již několik let utvrzují postupně zveřejňované bezpečnostní slabiny prakticky většiny známých WWW serverů. Bohužel na řadu těchto problémů lze aplikovat přirovnání ke „kostlivci ve skříni“, o kterém nevíte, kdy „ze skříně vypadne“. Pro ilustraci: chyba v Microsoft IIS, kterou zneužívá virus CodeRed pro své šíření existuje v tomto software již více než 5 let !! (od verze Windows NT 4.0, navíc stejná chyba byla „importována“ i do Windows 2000 – odhalena byla až v červnu 2001), tudíž pravděpodobnost, že v daném WWW serveru bude alespoň ještě jedna taková fatální chyba hraničí téměř s jistotou. Nejedná se ovšem pouze o problém zmíněné platformy, podobnou úvahu lze aplikovat i na řadu jiných produktů.

Výše uvedené problémy jsou v řadě případů navíc umocněny nepříliš zdařilým návrhem architektury samotného WWW serveru, který je často zcela zbytečně provozován s vysokými privilegii (root, system, administrator) nebo je dokonce téměř integrován do samotného operačního systému (což jen násobí případné následky zneužití přítomné bezpečnostní slabiny).

Všechny zmíněné okruhy problémů související s WWW servery je třeba mít na paměti při výběru technologie pro konkrétní řešení. Bezpečnostní problémy ovšem nemusí být problémem samotného WWW serveru, ale mohou být způsobeny chybou v provozované aplikaci – zejména v případě dynamických WWW stránek (skripty – ASP, PHP, Perl aj.) – z vlastní zkušenosti vím, že často naprosto běžný uživatel, naprosto obyčejným prohlížečem při troše experimentování s parametry v URL může dosáhnout „nečekaných výsledků“ (přístup k cizím datům apod.). Jelikož většina těchto aplikací je unikátním dílem pro konkrétního zákazníka, je velmi obtížné tyto slabiny odhalovat, zde doporučujeme rozhodně nepodcenit nejen důkladné testy funkčnosti, ale i zátěžové tresty, penetrační testy, eventuelně nezávislý audit zdrojových kódů.

4. Do bezpečnosti jsme zainvestovali – nyní jsme bezpeční

Ačkoli to bude možná znít trochu jako fráze, rád bych zdůraznil, že absolutní (100%) bezpečnost je pouze meta, ke které se můžeme blížit. Bezpečnost je pochopitelně také o penězích (investicích), ale nejen o nich. Bezpečnost nelze jednorázově pořídit, jedná se o kontinuální činnost, která vyžaduje jisté finanční, technické i lidské zdroje.

Problematiku bezpečnosti je přitom třeba vnímat ve dvou rovinách, jednak v rovině technických opatření (ty lze většinou „koupit“), ale také opatření organizačních (lidský faktor je vždy jedním z největších rizik, které nelze plně ošetřit technickým opatřením).

Dosavadní vývoj zmíněný v úvodu tohoto textu jednoznačně ukazuje, že je prakticky nemožné pořídit technologii (obzvlášť hovoříme-li o WWW aplikaci), která bude bez dalších zásahů např. několik let odolná vůči útokům z Internetu. Zcela nepochybně bude s postupem času zveřejněna řada oprav, patchů, hotfixů aj., které bude nutno instalovat,

lze rovněž očekávat opravy provozované WWW aplikace, může se stát, že výrobce některé použité komponenty (WWW server, databázový server) přestane dále podporovat Vámi provozovanou verzi atd. atd. Všechny tyto a podobné skutečnosti budou prakticky neustále znamenat dodatečné nároky na finanční zdroje (platby za support k jednotlivým produktům, externí služby apod.) a lidské kapacity, a to i v případě kdy nebudete nijak dramaticky rozvíjet funkčnost původního řešení.

5. Drahá technologie = dobrá (bezpečná) technologie

Přestože lze očekávat jistou míru korelace mezi cenou a kvalitou používané technologie, určitě nelze od ceny jednoduše odvodit úroveň její bezpečnosti. Podobně nelze tvrdit, že všechny technologie jistého výrobce jsou bezpečnější než technologie výrobce jiného.

Na základě vlastní zkušenosti si dovolím konstatovat, že drtivou většinu solidních, zavedených technologií (a nejen v oblasti související s WWW aplikacemi) lze provozovat způsobem, který poskytuje rozumnou úroveň bezpečnosti, a to bez ohledu na jejich cenu či výrobce. Většina těchto technologií poskytuje poměrně širokou škálu bezpečnostních parametrů, nastavení přístupových práv, zaznamenávání (auditu) klíčových událostí apod., které však často zůstávají nevyžity. Při výběru technologie doporučuji zaměřit pozornost na schopnosti dodavatele a přidané služby, které spolu s produktem nabízí než na technologii samotnou.

Asi netřeba dlouze vysvětlovat skutečnost, že i špičkovou vysoce bezpečnou technologii lze provozovat „nebezpečným“ způsobem, je-li tato technologie neodborně nainstalována nebo není-li věnována dostatečná odborná pozornost jejímu provozu a údržbě. Zde je vždy potřeba dobře zvážit, bude-li provozovaná technologie instalována a spravována vlastními zaměstnanci (v tom případě, je třeba při výběru technologie vhodné zohlednit zaměření a know-how těchto pracovníků) nebo externím dodavatelem – outsourcing (zde není volba technologie až tak podstatná, rozhodující bude celková kvalita nabízených služeb, poskytnuté garance apod.).

6. Používáme nejlepší technologie, patche máme, monitoring provádíme

Díky velmi dynamickému rozvoji a rychle rostoucí složitosti v současnosti provozovaných technologií (platí o WWW serverech, operačních systémech i dalších) lze bohužel jen velmi těžko hledat jistotu bezpečnosti. Jak již bylo dříve řečeno, složité systémy obsahují chyby (o některých z nich doposud bohužel ani nevíme), výrobci těchto systémů nás prakticky pořád budou „nutit“ k instalování oprav a patchů příp. k přechodu na novější verze – prakticky nekonečný cyklus.

Tento překotný rozvoj prakticky znemožňuje provádět jakékoli věrohodné certifikace bezpečnosti používaných technologií. Certifikace se totiž stává tak náročná, že se z praktického hlediska trvá déle než je životnost posuzované aplikace (systému), která je mezitím nahrazena novější verzí. Často jsou bohužel na trh uváděny technologie nepříliš odladěné, obvyklou příčinou bývají různé konkurenční tlaky („musíme být rychlejší než konkurence“), což se pochopitelně odráží i v úrovni jejich zabezpečení.

V poslední době se navíc některé bezpečnostní problémy stávají „soubojem o čas“, neboť po zveřejnění kritické bezpečnostní slabiny v systému, který provozujete, jste často postaveni před otázku, bude-li rychlejší výrobce s patřičným patchem nebo si Váš server „najde“ nějaký hacker (pochopitelně můžete server odstavit, ale za to zřejmě příliš ocenění nesklidíte). Tento „souboj o čas“ se stává zajímavější s nástupem různých automatů a „útočících červů“, kteří bývají vypuštěni do Internetu několik málo dní po zveřejnění bezpečnostní slabiny, kterou využívají k napadení a dalšímu šíření. Navíc existují poměrně věrohodné teorie diskutující, jakým způsobem lze takového červa „vypustit“ a „šířit“, aby v průběhu několika dní prohledal drtivou většinu IP adres veřejně přístupného Internetu.

Také je vhodné připomenout, že i v současné době existují typy útoků, proti kterým se prakticky nelze bránit. Mám tím na mysli např. tzv. DDoS útoky (Distributed Denial of Service) spočívající v zahlcení serveru či jedné konkrétní služby, a to způsobem, kdy

k zahlcení dochází díky enormnímu počtu požadavků pocházející až z několika stovek uzlů ovládaných útočníkem (právě tato distribuovanost velmi ztěžuje odhalení a filtrování těchto útoků). Přestože cílem tohoto typu útoku není ovládnutí serveru ani získání dat, může mít i samotná nedostupnost serveru velmi negativní dopady pro jeho provozovatele.

7. Útočník nemá šanci získat přístup k „ostrým“ provozním datům

Často se v praxi setkávám s podobným tvrzením – „firewall do vnitřní sítě nikoho nepustí, externí firma dohlíží firewall 24h denně“, „data máme uložena v databázi, kde jsou nastavena přístupová práva“, „z WWW aplikace se přistupuje pouze k replice ostrých dat“ atd. atd.

Proti výše uvedeným tvrzením lze těžko něco namítat nebo je obecně zpochybňovat, každopádně z vlastní zkušenosti vím, jak může např. jediná extranetová WWW aplikace umístěná do velmi kvalitně zabezpečeného internetového připojení vytvořit velice tenkou a křehkou překážku mezi hackerem v Internetu a „ostrými“ daty v interní databázi (v daném případě byl z Internetu otevřen pouze jediný port 443 – HTTPS na inkriminovaný WWW server s extranetovou aplikací, který stačil nejen k tomu, aby bylo možno WWW server ovládnout, ale také k získání přístupu do databáze – což v daném případě odhalil penetrační test nikoli skutečný útočník).

Obecně si dovolím tvrdit, že jakákoli aplikace zpřístupňující citlivá data z provozní databáze (byť jen na čtení) uživatelům přes Internet je potenciálně zneužitelná pro neoprávněný přístup k těmto datům. Při pokusu o průnik k takto citlivým datům se útočník rozhodně nebude pokoušet o přímé spojení z Internetu do databáze ve vnitřní síti, ale pravděpodobně se pokusí nejprve napadnout WWW server (ten je z Internetu přístupný), bude-li úspěšný získá šanci se pokusit o přístup k databázi z napadeného WWW serveru (spojení WWW server → databáze je povoleno). Samozřejmě nebude to tak jednoduché, narazí na autentizační mechanizmus (může se ovšem jednat o oprávněného uživatele pokoušejícího se o eskalaci svých práv), aplikace nepřistupuje k ostrým datům, ale pouze k jejich replice – zde je otázkou, jestli se případná neoprávněná modifikace dat jednoduše nezreplikuje do ostrých dat, analogicky by se dalo v podobných úvahách „co by, kdyby“ pokračovat dál. V podobných případech velmi doporučuji tyto a podobné aspekty a rizika velmi pečlivě analyzovat a zvážit dopady případných bezpečnostních incidentů a na jejich základě navrhnout adekvátní řešení.

8. Bez hesla se do naší WWW aplikace nikdo nedostane

Autentizace je rozhodně jednou z velmi významných oblastí při návrhu WWW aplikací. Nutno si však uvědomit, že autentizaci lze provádět různými metodami (jméno+heslo, certifikát, HW token) na různých úrovních (WWW server, WWW aplikace), přičemž ne vždy musí být tento mechanizmus tak odolný, jak očekáváte.

Řadu bezpečnostních slabin WWW serverů je ovšem možno zneužít k průniku, přestože provozovaná aplikace vyžaduje autentizaci. Po ovládnutí WWW serveru je útočník schopen v řadě případů poměrně elegantně buď přímo nasimulovat oprávněného uživatele, nebo získat a rozluštit některá zašifrovaná hesla, nebo „počkat“ na přihlášení opravdového uživatele a odchytit jeho heslo (závisí na konkrétní architektuře aplikace).

Přestože v případě šifrované komunikace je prakticky nemožné odchytit heslo v průběhu komunikace, je dobré uvážit i jiné hrozby podobného charakteru, jako např. odposlechnutí klávesnice na pracovní stanici uživatele (obzvlášť pokud používá sdílený počítač, počítač v internetové kavárně apod.).

Podobně je vhodné důkladně zvážit např. možnosti útoků na heslo hrubou silou (ať už on-line pokusy o přihlášení, tak off-line rozluštění zašifrovaných hesel – vzhledem k běžně dostupné výpočetní síle je úspěšnost překvapivě vysoká).

Nejmodernější autentizační metody využívající HW předměty – tokeny (generátory jednorázových hesel apod.) jsou z formálního hlediska „neprolomitelné“ i zde ale existují hrozby jako např. „převzetí relace“ – uživatel se přihlásí za pomocí svého HW tokenu,

útočník vhodnou metodou převezme již ověřenou relaci uživatele a jeho jménem může být schopen neoprávněně provádět některé operace.

9. Proč by se nás někdo pokoušel napadnout?

Samozřejmě některé instituce jako například banky nebo významná ministerstva jsou z podstaty „zajímavým terčem“, u řady jiných podniků se lze ovšem často setkat s podobným názorem.

Motivace útočníka může být mnohdy i nečekaná:

- Nejčastěji bude motivací pravděpodobně zviditelnit se (typicky výměna úvodní WWW stránky) – v těchto „mediálních“ případech obvykle největší újmou poškození image.
- V některých případech je napadený systém „pouze“ zneužit jako přestupní stanice pro další útoky (tj. role prostředníka), nebo je zneužit pro šíření souborů s pochybným obsahem apod.
- Cílem může být získat informace (ne nutně pro potřeby útočníka), provést nějakou operaci jménem někoho jiného, pozměnit data ve prospěch svůj (či jiného), získat (pro někoho) konkurenční výhodu – tento typ útoku lze považovat za jakousi cílenou kriminální činnost, obvykle není snahou útočníka se zviditelnit, spíše naopak zahladit stopy. Objektivně řečeno, bývá podstatně jednodušší zvolit pro tento účel nějakou sociálně inženýrskou metodu a dosáhnout cíle prostřednictvím zaměstnance dotyčné společnosti.
- Paradoxně může být motivací některých útoků jakási odplata za příliš dobře zabezpečený systém – např. útočníkovi se nedaří díky bezpečnostním opatřením aplikovat „nacvičený“ způsob průniku, a proto se uchýlí k pokusu o zahlcení serveru distribuovaným DDoS útokem.
- Bohužel v poslední době se můžeme setkat také s různými formami automatizovaných útoků – jednoúčelové scannery vyhledávající např. WWW servery jistého typu, o němž je známa bezpečnostní „díra“, po nalezení takového serveru okamžitě následuje pokus o jeho kompromitaci a nainstalování další instance scanneru a další šíření (podobným způsobem se šíří např. CodeRed, Nimda). Těmto automatickým scannerům je pochopitelně zcela lhostejné, jestli napadají WWW server banky, významného ministerstva nebo charitativní nadace.

Několik dobrých rad pro zabezpečení WWW aplikací

V této kapitole je zmíněna řada oblastí, které považujeme za podstatné při návrhu bezpečné WWW aplikace. Řada poznatků přímo reaguje na problematické okruhy zmíněné v předchozí části textu, řada z nich je poněkud obecnějšího charakteru a je aplikovatelná nejen v případě zabezpečení WWW serverů.

Bezpečnost základní infrastruktury

Kvalitně zabezpečená síťová infrastruktura je naprosto nezbytným stavebním kamenem. V této oblasti je potřeba velmi pečlivě volit síťovou topologii, do které bude WWW aplikace umístěna, pochopitelně sem spadá také odborně nainstalovaný a provozovaný firewall doplněný eventuelně o některé detekční systémy (IDS).

V otázce volby konkrétní technologie velmi doporučujeme zohlednit solidnost, kvalitu a odborné zázemí dodavatele, stejně jako přidané služby, které spolu s dodávkou této technologie nabízí (mezi nejpodstatnější patří support, monitorování/dohled jednotlivých zařízení apod.).

Obecná doporučení z této oblasti:

- doporučujeme striktně oddělit funkci firewallu jako filtru a aplikační brány, neboť existuje nezanedbatelné riziko zneužití chyby v SW některé z aplikačních bran

k následnému průniku na firewall, čímž získá útočník kontrolu nad samotným filtrovacím mechanizmem

- doporučujeme v maximální možné míře separovat jednotlivé servery do samostatných demilitarizovaných zón, a tak eliminovat riziko zprostředkovaného útoku
- pokud možno se vyvarovat kombinování několika aplikací (např. DNS+SMTP+WWW) na jediném serveru, současné operační systémy bohužel neumožňují tak důsledné oddělení jednotlivých provozovaných aplikací, aby kompromitace jedné z nich neohrozila ostatní
- nepodcenit nutnost korektního nastavení systému, administrace a údržby systému (monitoring, kontrola, instalace oprav, upgrade apod.)

Bezpečnost vlastního WWW serveru

Ačkoli to může znít trochu „demagogicky“, doporučuji při úvahách o architektuře WWW aplikací již dopředu počítat s tím, že WWW server může být přes veškerou Vaši snahu s poměrně vysokou pravděpodobností „úspěšně“ napaden. Tento poněkud tvrdý přístup je ovšem založen na praktických poznatcích (WWW server, který je dnes považován za bezpečný, může být za měsíc naprosto fatálně zranitelný, aniž byste s ním cokoli provedli).

- na samotném WWW serveru doporučujeme pokud možno nedržet žádná cenná data, a to včetně citlivých informací jako jsou přístupová jména a hesla (byť v zašifrované podobě)
- nejenže nedoporučujeme kumulovat funkci WWW serveru a databáze, ale dokonce doporučujeme komunikaci s databází omezit tak, aby ani v případě plného ovládnutí WWW serveru nebyl útočník schopen klást libovolné SQL dotazy (což lze řešit např. voláním uložených procedur v databázi)
- je-li to možné a finančně únosné je vhodné pro účely WWW aplikací zveřejněných do Internetu realizovat repliky provozních databází (do takové repliky lze např. umístit pouze nezbytné minimum dat a tím snížit související rizika).

Výběr technologie a návrh WWW aplikace:

- přestože jsem v předchozím textu uvedl, že volba technologie není až tak podstatná, neboť většinu solidních produktů lze provozovat bezpečně, rád bych současně na tomto místě doporučil vyvarovat se „chronicky problémovým“ technologiím
- jako vlastní WWW server doporučujeme zvolit některý z robustních zavedených WWW serverů (Apache, iPlanet/Netscape, Lotus Notes příp. MS IIS), obecně doporučuji vyvarovat se použití různých speciálních, v praxi nepříliš rozšířených a často ne příliš kvalitně odladěných WWW nadstaveb databázových systémů (jako např. WebDB, iReach) – tyto technologie často trpí řadou nedostatků, které sice neohrožují přímo jejich bezpečnost, ale umožňují znepřístupnění příp. zhroucení celé služby.
- v otázce šifrování není prakticky o čem přemýšlet, jsou-li přenášena jakákoli neveřejná data rozhodně doporučujeme šifrovat (protokol HTTP over SSL podporují všichni výrobci zavedených WWW serverů)
- v otázkách použitého způsobu autentizace budou patrně významnou roli hrát finanční prostředky, poněvadž prakticky nejbezpečnější autentizační metody využívající HW předměty – tokeny jsou poměrně nákladnou záležitostí, zde je potřeba v konkrétním případě zvážit tyto investice spolu s riziky, která by přinesla jiná autentizační metoda (SSL certifikát příp. uživatelské jméno+heslo).
- v rámci nasazování WWW aplikací je nutné dodržovat stanovená pravidla pro vývoj aplikace, změnové řízení a nasazování nových verzí (tyto aplikace bývají často nasazovány pod časovým tlakem – ztráta konkurenční výhody apod.)
- při návrhu WWW aplikací je nutné mít na paměti, že potenciální rizika neleží výhradně na straně serveru, ale rovněž na straně klientů (WWW prohlížeč), z tohoto důvodu

doporučujeme velmi pečlivě vážit ukládání různých informací o uživateli prostřednictvím tzv. cookies, dále je vhodné zvážit rizika plynoucí z kompromitace (odcizení) pracovní stanice uživatele.

Závěr

Cílem, tohoto příspěvku bylo především poskytnout posluchačům alespoň část autorových praktických poznatků z oblasti auditů a penetračních testů nejen WWW aplikací. Pevně věřím, že tato forma sdílení zkušeností bude pro posluchače zajímavá a přínosná.