David Ondřich

# ArcIMS a bezpečnost

## Část první

Tímto článkem zahajujeme sérii článků o zabezpečení ArcIMS serveru, služeb a bezpečném poskytování dat. Série navazuje na přednášku o bezpečnosti a ArcIMS ze 14. konference uživatelů GIS ESRI a Leica Geosystems a podstatným způsobem ji rozšiřuje a doplňuje.

## Úvodem

Seriál je čtyřdílný, připravte se proto na relativně dlouhé čtení. Každý článek ze seriálu by měl být plnohodnotným informačním zdrojem, ačkoliv se mezi jednotlivými články intenzivně odkazuji a pokud se chce čtenář zabývat problematikou bezpečnosti podrobněji, měl by si články přečíst všechny. Seriál je ovšem třeba chápat pouze jako úvod k dalšímu studiu obecných bezpečnostních pravidel.

První a poslední část seriálu bude poněkud více „povídací“, prostřední dvě části budou zaměřeny technicky a k jejich pochopení je nutné, aby se čtenář orientoval ve vlastnostech a schopnostech ArcIMS serveru. V první části se zaměříme na obecné poznámky, které se týkají bezpečnosti, běžně používané strategie a postupy a zejména se soustředíme na doporučení týkající se ArcIMS a popíšeme si architekturu ArcIMS. Toto architektonické schéma pak rozvedeme v druhé části, kde se zaměříme na zabezpečení ArcIMS serveru jako takového, ukážeme si různá bezpečnostní paradigmata a konfiguraci ArcIMS serveru v složité heterogenní síti; povíme si také něco o možných typech útoků na ArcIMS. Ve třetí části se pěkně zblízka podíváme na zabezpečení dat publikovaných prostřednictvím ArcIMS, řízení přístupu uživatelů k datům a službám a shrneme problémy, které datům a službám v nepřátelské síti hrozí. Ve čtvrté části se zaměříme na důsledky, které může vyvolat napadení ArcIMS serveru, některé související právní důsledky a pokusíme se shrnout celý seriál a zhodnotit celkové schopnosti ArcIMS z pohledu bezpečnosti.

## O bezpečnosti obecně

Jako ve všech oborech i zde platí, že nejlepší je nechat prostor odborníkům, ovšem každý správce serveru by měl znát určité „bezpečnostní minimum“, proto nezaškodí, když si několik základních pravd připomeneme.

Základní tvrzení o počítačové bezpečnosti by se dalo shrnout do (poněkud zavádějící) věty, že bezpečnost vlastně neexistuje, resp. že stoprocentní bezpečnosti nelze nikdy dosáhnout. Často se též říká, že bezpečnost není stav, ale nikdy nekončící proces. Obě věty jsou pravdivé v tom smyslu, že i pro sebelépe zabezpečený systém existuje jistá nenulová pravděpodobnost, že se do něj podaří útočníkovi proniknout, nebo – to mnohem častěji – že se systém z důvodu vnitřní chyby nebo špatné konfigurace zhroutí (a poškodí např. některá data). Odborníci většinou říkají, že má smysl uvažovat o úrovních zabezpečení a jejich nákladnosti, velmi vysoká míra zabezpečení obvykle vyžaduje velmi vysoké náklady a s výjimkou informací podléhajících nejvyššímu utajení se zpravidla ukáže, že pro tak vysokou míru bezpečnosti není dostatek prostředků.

Druhým důležitým prvkem bezpečnosti je cosi, co se obvykle označuje jako strategie. Ačkoliv to zní velmi honosně a ve velkých firmách na toto téma občas existují podrobné a rozsáhlé předpisy, obvykle stačí, když existuje psaný (nebo hůře nepsaný) úzus o tom, jaká jsou základní bezpečnostní pravidla v dané organizaci. Většinou by měl o těchto pravidlech mít ponětí systémový administrátor, vedoucí IT oddělení, případně někdo další. Tato obecná pravidla by měla stanovit, které základní bezpečnostní mechanizmy se používají, kde a proč, případně jaké jsou z nich výjimky. Největším problémem takové strategie nebývá ji vytvořit (i když ve větší firmě může být problém skloubit mnohdy zcela protichůdné požadavky jednotlivých oddělení), ale především ji dodržovat. Strategie by proto měla obsahovat jednoduchá, jasná a snadno zapamatovatelná pravidla („hesla nelepíme na papírcích zboku na monitor“). Součástí strategie by také měla být jistá předvídavost, jak se chovat v případě, že dojde k nějakému porušení bezpečnosti. Když tyto poznámky existují i v nějaké písemné (elektronické) podobě, může se to leckdy hodit. Další poznámky k tomuto tématu najde čtenář v poslední části seriálu.

Součástí strategie by rozhodně mělo být základní rozhodnutí, jak se bude přistupovat k bezpečnosti: maximalisticky, nebo minimalisticky? V anglické literatuře se toto dilema označuje jako *allow, deny* vs. *deny, allow* a znamená v podstatě rozhodnutí, zda je povoleno vše, co není zakázáno (první přístup), nebo zda všechno, co není explicitně povoleno, je zakázáno (druhý přístup). Oba přístupy mají své opodstatnění. U každého druhu zabezpečení je dobré se zamyslet, který způsob je lepší; ne vždy je vhodné používat v praxi dosti častý postup „je jednodušší všechno povolit a pár drobností zakázat, proto to tak uděláme“.

Jednou z nejdůležitějších informací, kterou byste si měli z tohoto seriálu odnést, je, že největší bezpečnostní riziko každého systému představují jeho uživatelé (a správci, kteří jsou speciální skupinou uživatelů). Tato obecná pravda je často zcela opomíjena, ačkoliv se ví, že za drtivou většinou úspěšných průlomů do počítačových systémů stojí především tzv. *social engineering*, tzn. manipulace s uživateli systému a jejich vědomá či nevědomá spolupráce s útočníkem.

V souvislosti s uživateli je třeba připomenout ještě jednu důležitou věc, a tou je fyzické zabezpečení systému. Je pěkné, když má organizace důležité servery a datové zdroje důsledně odděleny v samostatných sítích na jiných fyzických linkách odděle-

ných směrovači a firewally, aby se k nim po síti téměř nebylo možné dostat. Jenže co je to platné, když všechno „sedí“ v jedné klimatizované serverovně, která je za společnými dveřmi s místností pro uklízečku, opatřenými jedním obyčejným zámkem. Vytáhnout z diskového pole harddisk nebo odnést malý server trvá zkušenému zloději několik sekund a pokud je dostatečně drzý, vrátný mu ještě podepíše zápůjční list. Cena hardwaru pak obvykle není tím, co firmu bude trápit ze všeho nejvíc.

Poslední důležitý bod, o kterém je zapotřebí se zmínit, souvisí s hlídáním systému, který chceme zabezpečit. Dostatečný monitoring a znalost chování uživatelů i systému je základním předpokladem, který umožňuje ověřovat, že stanovená bezpečnostní pravidla fungují, případně vytvářet na základě konkrétních poznatků nová. Obvyklým způsobem tohoto monitoringu je logování uživatelských akcí, požadavků na webovou aplikaci apod., ale také se často využívají metody přímého sledování, automatického zasílání zpráv (např. na mobilní telefon) ad. Ačkoliv v běžném provozu bývá obvykle těžké věnovat pravidelnému sledování dostatečnou prioritu, v případě reálného bezpečnostního incidentu může detailní znalost normálního chování systému pomoci administrátorovi odhalit problém již ve velmi raných stádiích (a předejít tak horším následkům).

## Únikový východ

Název této části tak trochu navozuje představu cesty, kterou ve skutečnosti nikdy nebudete chtít použít. Také ovšem označuje jisté bezpečnostní minimum, které musí splňovat každá budova. Podobné je to s informačními systémy, každý by měl splňovat jisté základní předpoklady, bez nichž by vůbec neměl být spuštěn. Pojďme se podívat na taková minimální opatření v případě ArcIMS serveru.

- *Pokud je to možné, použijte pro ArcIMS dedikovaný server.* Ačkoliv to zní jako triviální rada, je to poměrně důležitá zásada. Není nutné na ní lpět, někdy prostě není možné pro danou úlohu získat samostatný hardware (např. z výkonnostních nebo finančních důvodů), nicméně pokud tomu nebrání žádný vážný důvod, snažte se pro provoz mapových služeb použít samostatný stroj. Více se k tomuto tématu vrátíme ve druhé části.

- *Zakažte všechno, co nepotřebujete.* I tohle je jednoduchá rada, kterou je ovšem třeba stále připomínat. Na serveru, kde poběží ArcIMS, povypínejte všechny systémové služby, které nepotřebujete (sdílení disků, tiskáren, telnet démon nebo vzdálený přístup na X Window Server). I k tomuto tématu se ještě vrátíme ve druhé části.

- *Nenechávejte počítač na větru a dešti.* Použijte firewall, minimálně nějaký softwarový, mnohem lépe samostatný firewall, v ideálním případě ve spojení s routerem, který vytváří demilitarizovanou zónu (DMZ). Svět „tam venku“ je poměrně divoký, firewall už dnes naštěstí představuje samozřejmou základní ochranu jakéhokoliv počítače připojeného k internetu.

- *Držte prst na tepu doby.* Aktualizujte, záplatujte, aplikujte opravy. To se netýká jen samotného ArcIMS, ale i operačního systému a dalšího softwaru. Prakticky všechny serverové systémy již dnes disponují nějakým automatickým zjišťováním, zda jsou dostupné aktualizace a záplaty, většinou se po administrátorovi chce pouze to, aby odsouhlasil jejich stažení a aplikaci (u systémů Microsoft Windows je občas nutný restart, počítejte s tím při plánování času na údržbu systému). Sledujte literaturu o novinkách ve světě bezpečnosti; na internetu najdete řadu magazínů o bezpečnosti (doporučuji sekci Security News na serveru www.crypto-world.info).

Kromě těchto základních pravidel platí řada dalších obecných zásad. Rozmyslete si, jak vypadá cílová skupina uživatelů vašeho systému. Chcete, aby systém používal kdokoli z celého světa? Bude uživatelů skutečně jen jedna skupina? Téměř vždy se vyplatí zavést pravidla pro autentizaci (ověřování identity) a autorizaci (udělování práv např. ke službám nebo úkonům) uživatelů. Obvykle už v organizaci existuje nějaký systém pro autentizaci a autorizaci uživatelů, pak je možné s ním server propojit a využít výhod sdíleného zdroje. Pro internetové uživatele pak můžete vytvořit anonymní účet, nebo (lépe) zpřístupnit jim jen některé služby.

Publikujte jen to, co opravdu chcete nebo musíte, a publikujte to jen pro správné uživatele. Sice se stává zřídka, že by někdo omylem publikoval mapovou službu s daty, kterou ve skutečnosti publikovat nechtěl, nicméně snadno se může stát, že správce zapomene např. zrušit mapovou službu, která poskytovala časově omezená data.

Poslední obecná rada se opět týká předpokládané bezpečnostní strategie. Pro daný server si stanovte základní priority a zvažte možná rizika. Opět se hodí tužka a papír a jeden pár očí navíc, který možná upozorní na něco, co jste přehlédli. Potřebujete, aby server běžel skoro pořád? Nebo potřebujete, aby byl co nejbezpečnější? Nebo naopak chcete, aby jeho provoz byl co nejlevnější? Co se stane, když v důsledku pádu systému nebo bezpečnostního incidentu hodinu (den, týden) nepoběží? Takové jednoduché otázky velmi pomohou ujasnit, co je vlastně skutečně důležité (a v rámci dostupných zdrojů možné).

## Anatomie ArcIMS

K tomu, abychom mohli v příštím díle začít uvažovat o vhodném uspořádání ArcIMS serveru, je nutné, abychom měli poměrně detailní znalost jeho vnitřní architektury. Ta je v jádru jednoduchá, přesto může být v některých konfiguracích zdrojem (nemilých) překvapení. Každý ArcIMS server představuje několik komponent, které navzájem spolupracují.

Tyto komponenty si můžeme představit jako jednotlivé vrstvy, kterými prochází požadavek na mapový server shora dolů, zatímco odpověď serveru na tento požadavek těmito vrstvami naopak prochází zdola nahoru. Každá z vrstev si z požadavku

vytáhne informace, které potřebuje, a předá požadavek další vrstvě, naopak při cestě zpět se k odpovědi v každé vrstvě přidávají další informace (pokud je to potřeba).

Každý ArcIMS server sestává z pěti vrstev, z nichž nejvrchnější a nejspodnější vlastně nejsou přímo součástí ArcIMS, nicméně pro úplnost a zejména pro budoucí rozvržení bezpečnostní politiky je do výčtu zahrneme. Z pohledu shora (tedy tak, jak přichází požadavek) jsou to 1) webový server, 2) konektor, 3) aplikační server, 4) výkonná vrstva (Spatial Server) a 5) datová vrstva. Každou z těchto vrstev si dále podrobně popíšeme a vysvětlíme, jaká je její úloha v řetězci zpracování požadavku.

1. **Webový server.** Po operačním systému je to první software, který přijde do styku s požadavkem, který dorazil na mapový server. Značnou část požadavků vyřídí, aniž by je předával nižším vrstvám (chyby, požadavky na navigační grafiku použitou v prohlížeči apod.), pouze konfiguračně vymezenou část požadavků přepošle další vrstvě, konektoru. Webový server není součástí ArcIMS a je také hlavním zdrojem log souborů o požadavcích, které na server přišly. Obvykle se používá Apache HTTP Server (Apache) nebo Microsoft Internet Information Server (IIS). Jako komunikační protokol používá HyperText Transfer Protocol (HTTP).

2. **Konektor.** Konektor spojuje webový server s vrstvou aplikačního serveru. Jeho hlavní úloha spočívá především v kontrole požadavku, zda odpovídá dohodnutému „jazyku“, případně provádí autentizaci/autorizaci uživatelů a kontroluje výskyt povolených klíčových slov v požadavku. Standardním konektorem je tzv. *servlet konektor*, který umožňuje komunikaci s okolním světem v jazyce ArcXML, tento konektor má široké konfigurační možnosti a poskytuje většinu funkcí, které jsou obvykle na ArcIMS kladeny (použitá technologie servletů navíc umožňuje jeho schopnosti programově rozšiřovat). Dalšími obvyklými konektory jsou WMS a WFS konektory, které zajišťují komunikaci v dobře definovaných protokolech. Součástí vývojářských nástrojů pro ArcIMS jsou i knihovny pro programování vlastních konektorů (Java, ASP, ColdFusion, částečně i .NET), které dávají prostředky pro zakomponování ArcIMS do jiných informačních systémů. Konektor na vstupu komunikuje prostřednictvím HTTP (na nízké úrovni) a příslušného „jazyka“ (ArcXML, WMS, WFS), na výstupu komunikuje s aplikačním serverem prostřednictvím ArcXML.

3. **Aplikační server.** Aplikační server (AS) je hlavní řídicí jednotkou ArcIMS, který podle typu požadavku a podle zatížení výkonné vrstvy rozděluje práci na příchozích požadavcích výkonné vrstvě. (AS je součástí ArcIMS, jeho název se někdy zaměňuje s webovým aplikačním serverem, který je hostitelským prostředím pro konektor [viz výše] – nebude-li uvedeno jinak, znamená zkratka AS nebo označení „aplikační server“ střední vrstvu ArcIMS.) AS funguje jako manažer, který řídí práci jednotlivých výkonných jednotek, sleduje jejich vytíženost a podle ní přiděluje zpracování jednotlivých požadavků. Jeho konfigurací se ovlivňuje výkon celého ArcIMS. Na vstupu a výstupu komunikuje pomocí ArcXML.

4. **Výkonná vrstva.** Pokud je AS mozkem ArcIMS, pak výkonná vrstva představuje srdce, jádro celého systému. V této vrstvě se požadavek zpracuje do podoby odpovědi, která se odešle zpět uživateli (klientu), ať už je to v podobě vykreslení mapy, vyhledání údajů nebo provedení nějaké operace nad daty (např. buffer). Výkonnou vrstvu představuje jeden nebo více tzv. *spatial serverů* (SS). Každý SS je samostatným procesem v operačním systému, který běží na pozadí a AS s ním komunikuje síťovými prostředky. V jednom systému tedy může běžet více SS, potom se dělí o dostupné systémové prostředky (čas procesoru, paměť). Situace je ještě o něco složitější v tom, že každý proces může být (a téměř vždy také je) rozdělen do několika tzv. vláken, která pracují do značné míry nezávisle na sobě. Smyslem existence těchto vláken je zejména zvýšení výkonu a odezvy celého

serveru, z hlediska bezpečnosti to není tolik podstatné, proto nadále budeme uvažovat o každém SS jako o samostatném procesu, který zpracovává požadavky a kreslí mapky nebo vyhledává v datech. SS na vstupu používá ArcXML (teprve tady dojde ke zpracování, tzv. parsování celého požadavku, všechny předchozí vrstvy do požadavku pouze „nahlížely“, jestli v něm nejsou zajímavé informace), na „výstupu“ (v pravém smyslu se o výstup nejedná) používá podle příslušného datového zdroje buď přístup do souborového systému, nebo databáze.

5. **Datová vrstva.** Stejně jako webový server, ani datové zdroje nejsou v pravém smyslu součástí ArcIMS, pro dokreslení celkového obrazu a pro další potřeby je však uvažujeme jako nejnižší vrstvu. Data mohou být uložena buď v souborech (přímo na serveru nebo na nějakém sdíleném síťovém disku), nebo v databázi (pro naše potřeby nyní není důležité, o jakou databázi se jedná). Datová vrstva přímo nezpracovává žádný požadavek, ve skutečnosti se k žádnému vůbec nemá možnost dostat – všechny požadavky skončí na úrovni výkonné vrstvy. Datové zdroje pouze poskytují samotná data, která slouží pro vytvoření odpovědi na požadavek. Komunikace mezi SS a datovými zdroji se obvykle neomezuje jen na poskytování dat, ale většinou také na poskytování informací o samotných datech, např. při inicializaci ArcIMS serveru se SS ptá na rozsahy jednotlivých datových souborů apod.

Ve skutečnosti je nastíněná architektura ArcIMS poněkud složitější, nicméně pro potřeby úvah o bezpečnosti zcela vystačíme s uvedeným modelem, který navíc přímo vybízí k tomu, abychom začali experimentovat s rozmístěním jednotlivých vrstev. Poslední důležitá informace o architektuře ArcIMS je ta, že jednotlivé komponenty mohou být na fyzicky oddělených serverech, neboť spolu komunikují pouze síťovými prostředky – ačkoliv důvody pro tuto nezávislost jednotlivých částí jsou spíše výkonnostní, pro potřeby bezpečnosti se nám to bude velmi hodit, jak uvidíme již v příští části.

Všechny uvedené informace se týkají poslední verze ArcIMS, což je v době vzniku tohoto seriálu verze 9.1, většina jich ovšem platí i pro starší verze ArcIMS (od verze 4.0 dále) a s pravděpodobností hraničící s jistotou bude platit i pro připravovanou verzi 9.2.

## Pokračování příště

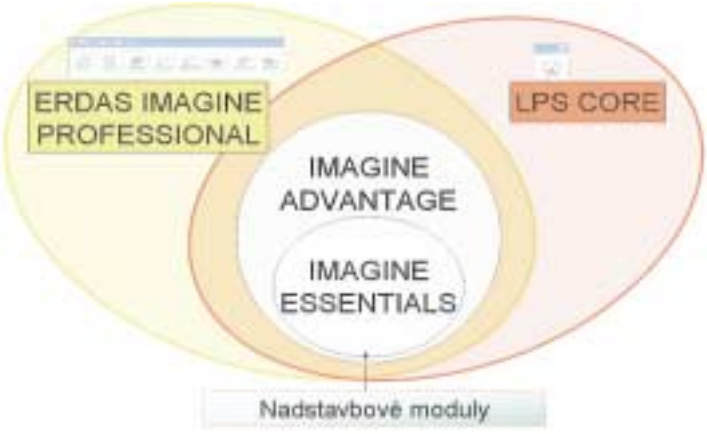
Následující díl bude podstatně více technicky zaměřen, zejména se budeme zabývat architekturou ArcIMS, resp. jak z hlediska bezpečnosti rozmístit jednotlivé vrstvy a jaké má ta která varianta vlastnosti. Podíváme se také na jednotlivé protokoly, kterými spolu vrstvy komunikují, potřebné porty, na kterých se navzájem poslouchají, a možnosti konfigurace součástí. Povíme si také něco o možnostech přímého sledování systému, o možných útocích na celý server a povídáním o rozlišování jednotlivých typů klientů si připravíme půdu pro třetí část.

*Mgr. David Ondřich, ARCDATA PRAHA, s.r.o.*

Inka Tesařová

# Aktuální verze a současná struktura software Leica Geosystems

Firma Leica Geosystems Geospatial Imaging, LLC nabízí širokou škálu produktů pro práci s geografickými rastrovými daty. Základní řadu software Leica Geosystems tvoří v současnosti:




*Architektura software Leica Geosystems*

- ERDAS IMAGINE 9.0 (verze 9.1 bude k dispozici od října 2006),
- LPS 9.0 (9.1 od října),
- Leica Virtual Explorer 3.1,
- Image Analysis a Stereo Analyst pro ArcGIS 9.1 (9.2 od prosince).

## ERDAS IMAGINE

Software ERDAS IMAGINE je zaměřen především na práci s leteckými a družicovými snímky – od vytvoření ortosnímků až po vyhodnocení informací o typu pokryvu, aktualizaci polohopisu a mapování výškopisu. Umožňuje pracovat s nejrůznějšími geografickými daty (i vektorovými) a je také připraven na řešení celé řady úloh GIS (např. prostorovou analýzu).