Eva STOPKOVÁ

BEZPEČNOSŤ ONLINE PUBLIKOVANIA DÁT

Stopková, E.: Security of online data publishing. Kartografické listy 2010, 18, 4 refs.

Abstract: The purpose of this thesis is to outline possibilities, how can be our data, published online, attacked and how to avoid conscious or unintended threats or damages of them. Functionality of computer system depends on cooperation of parts that can be attacked with purpose to disable system or obtain important information (for example data). It is important to know about risks and how to protect our computer or web service, but also to assess effectiveness and cost of possibilities in comparison with exposed data. Thesis deals also with security of publishing geodata, separate chapter refers to possibilities of stratification of users' privileges in access, view, editing and loading geodata. There are mentioned possibilities of stratification of viewing geodata based on different access privileges given by scale or resolution.

Keywords: threat, data privacy, data integrity, data accesibility, data autenticity

Úvod

Internet poskytuje široké možnosti publikovania dát z oblasti geoinformatiky. Informácie o dostupných dátach, ich kvalite a cene, môžeme získať formou publikovaných metadátových katalógov. Rastrové obrázky požadovaných dát sú dostupné prostredníctvom webových mapových služieb (WMS – Web Map Service), oproti tomu aktívnu prácu s priestorovými dátami umožňujú webové prvkové služby (WFS – Web Feature Service). Ďalej sú k dispozícií WCS (Web Coverage Service), webové služby, ktoré umožňujú prácu s rastrovými dátami typu digitálny model reliéfu, či družicové snímky, WPS (Web Processing Service), ktoré poskytujú geoprocesné funkcie a iné typy webových služieb. Výhoda publikovania dát nespočíva len v zjednodušení komunikácie medzi poskytovateľom a žiadateľom dát a v rozšírení možností, ako dáta vyhľadávať, porovnávať a získavať, ale aj v zefektívnení práce. Príkladom môže byť decentralizácia poskytovania dát, ktoré môžu byť poskytované inštitúciami v rôznych regiónoch, taktiež odpadá potreba fyzickej prítomnosti zamestnanca pri práci s dátami. Tieto výhody sú však spojené s viacerými rizikami, o ktorých pojednáva tento článok.

1. Zložky modelu sieťových procesov

Základom sieťových procesov je tzv. referenčný model OSI (Open System Interconnection Reference Model alebo Referenčný model prepájania otvorených systémov), ktorý pozostáva zo siedmich vrstiev (Endorf et al., 2005). Každá z týchto vrstiev má svoju špecifickú úlohu, avšak podstatou ich činnosti je, vlastnou funkcionalitou doplniť vrstvu bezprostredne nižšiu, a zároveň byť základom pre funkcionalitu vrstvy bezprostredne vyššej. Funkčnosť a bezpečnosť systému na publikovanie dát teda úzko súvisí s bezchybnou náväznosťou jednotlivých vrstiev, ale aj s včasným rozpoznaním rizík, ktoré sú pre každú vrstvu rôzne.

Fyzická vrstva zahŕňa komponenty prepojenia súčastí siete, t.j. fyzické vodiče, konektory, adaptéry a pod. Tieto musia spĺňať stanovené fyzické a elektrické štandardy, inak vzájomnou nekompatibilitou znemožňujú funkčnosť systému. Prenos dát fyzickou vrstvou je riadený prenosovými štandardmi linkovej vrstvy, založenými na bitovej špecifikácii a priebehu signálu prenosového štandardu (Endorf et al., 2005). Adresáciu dát, ich balenie do tzv. paketov, dodanie a formátovanie podľa požiadaviek linkovej vrstvy zabezpečuje sieťová vrstva. Spoľahlivosť jej činnosti je overovaná transportnou vrstvou, ktorá kontroluje súčty paketov a v prípade potreby vysiela príkaz na opakovanie prenosu.

Ing. Eva STOPKOVÁ, Slovenská technická univerzita, Stavebná fakulta, Katedra geodetických základov, Radlinského 11, 813 68 Bratislava, e-mail: eva.stopkova@gmail.com

Komunikácia a prenos informácií na vyššej úrovni (medzi programami, procesmi a používateľmi) sa odohráva v relačnej vrstve. To, ako sú dáta interpretované, spadá do kompetencií prezentačnej vrstvy, tvorenej rozhraniami aplikačných programov (API). Aplikačné programy využívajú na prácu s dátami protokoly aplikačnej vrstvy, napr. http (Hypertext Transfer Protocol, protokol na prenos textových stránok), FTP (File Transfer Protocol, protokol na prenos súborov).

Každý zo spomínaných protokolov môže byť zneužitý a dátam hrozí napadnutie v ktorejkoľvek z vrstiev modelu OSI. V nižších vrstvách je útok realizovaný napríklad pretečením pamäte, či sledovaním paketov a neautorizovanou manipuláciou s nimi. Vo vyšších vrstvách hrozí nedovolený prístup k adresárom s dátami, či zneužitie zoznamu s menami a prístupovými heslami. Niektoré hrozby útočia na viaceré vrstvy súčasne, napr. sledovanie klávesnice a odčítavanie zadávaných citlivých údajov. Je treba si uvedomiť zraniteľné miesta systému a zvážiť náklady potrebné na zamedzenie hrozieb tak, aby príslušné opatrenia boli účinné a zároveň adekvátne cene dát.

2. Bezpečný systém, riziká a možnosti ich eliminácie

V bezpečnom systéme je zaručené (Matiaško et al., 2004):

1. utajenie,
2. integrita,
3. dostupnosť,
4. autenticita.

V rámci *utajenia* sú aplikované opatrenia proti prehliadaniu dát neautorizovaným používateľom počas uchovávania dát v systéme, pri prenose alebo pri odovzdaní adresátovi. Tieto opatrenia môžu byť softvérové (zamedzenie sledovaniu siete, načítavania stláčaných kláves a pod.), ale aj také, ktoré minimalizujú škody spôsobené zlyhaním ľudského faktora (krádež, prezradenie citlivej informácie, zanedbanie opatrení na ochranu dát). Využívanou metódou na zabezpečenie utajenia dát je šifrovanie pri ukladaní dát alebo pri ich prenose, avšak aj pri šifrovaní netreba podceniť ostatné bezpečnostné riziká. Utajenie je takisto zabezpečené autorizáciou prístupu a overovaním používateľov.

Integrita dát zaručuje presnosť a zaručenosť ich obsahu. Riziko neautorizovanej úpravy dát sa znižuje správnou funkčnosťou hardvérových, softvérových a komunikačných prostriedkov a ochranou systému pred tzv. malwarom. Malware je súhrnné označenie počítačových vírusov, červov, trójskych koní a spywaru. Vírusy a červy sú programy, určené na záškodnícku činnosť v napadnutom počítači. Na infikovanie počítača červom, na rozdiel od vírusu, nie je potrebný ľudský zásah typu otvorenie infikovaného e-mailu, či inštalácia povolená používateľom. Spyware bez vedomia používateľa posiela dáta z jeho počítača. Môže byť maskovaný ako trójsky kôň, navonok vykonáva užitočnú činnosť, avšak v realite vykonáva záškodnícku činnosť. Okrem odosielania informácií značne spomaľuje chod počítača a môže prepisovať URL zadané v internetovom prehliadači. Spyware sa do počítača dostane len inštalovaním samotným používateľom. Proti týmto hrozbám je účinné chrániť sa pomocou antivírových softvérov a firewallu, ale dôležitá je aj prevencia. Netreba napr. otvárať e-maily od podozrivých odosielateľov (tieto e-maily sú väčšinou prijímané ako spam), avšak vždy je riziko, že infikovaný môže byť aj súbor od odosielateľa, ktorého považujeme za dôveryhodného. Taktiež je riskantné otvárať reklamné, či iné podozrivé webové stránky. Integrita dát môže byť narušená aj vlastnou chybou, či zlomyseľnosťou (napr. zmazaním konfiguračných súborov).

Dostupnosť dát zaručuje autorizovaný prístup k dátam. Kapacita systémov musí byť dimenzovaná na dostatočný výkon v danom čase. V prípade, že požiadavky na systém presiahnu kapacitu systému, môže dôjsť k jeho kolapsu, v horšom prípade k strate alebo poškodeniu dát. Riešením môže byť ponechanie dostatočnej rezervy alebo využitie redundantných mechanizmov. Táto metóda býva využívaná pri tzv. internetovom výpalníctve, kedy útočník zašle obeti obrovské množstvo požiadaviek. Realizuje to prostredníctvom tzv. zombie, počítačov infikovaných trójskym koňom alebo vírusom. Preventívne proti strate dát je osvedčené zálohovanie (online alebo offline), využívanie záložných zariadení pri výpadku systému a zaškolenie personálu na jeho opätovné uvedenie do prevádzky.

Autenticita dát zaručuje ich pravosť, pôvod a výpovednú hodnotu. V zásade, ak je zabezpečené utajenie a integrita dát, vytvorených relevantnou metodikou, ich autenticita nemôže byť narušená zvonku. Pri niektorých dátach sa na jej potvrdenie využíva elektronický podpis.

3. Špecifiká publikovania geodát

Prístup klienta k mapovému serveru, kde sú uskladnené dáta, je umožnený prostredníctvom rozhrania, ktoré umožňuje ich vzájomnú spoluprácu koordináciou štandardizovanými protokolmi OpenGIS konzorcia (OGC® Standards and Specifications, http://www.opengeospatial.org/standards). Mapy priestorových dát sú generované na základe geografickej informácie, ktorú zadáva klient svojimi požiadavkami. Ak je mapa doručená v rastrovom obrázkovom formáte (PNG, GIF, JPEG, TIFF atď.), hovoríme o webovej mapovej službe (WMS), avšak môžeme sa stretnúť aj s vektorovými výstupmi vo formáte SVG (Scalable Vector Graphics) alebo WebCGM (Web Computer Graphics Metafile). V prípade, že výstupom sú samotné dáta alebo ich časť, ide o webovú prvkovú službu (WFS).

Ako bolo naznačené v predchádzajúcich statiach, zdrojové dáta treba chrániť pred viacerými hrozbami. K už spomínaným rizikám, ktorým sú vystavené dáta vo všeobecnosti, patrí neautorizovaný prístup. Otázka prevencie sa dá vyriešiť viacerými spôsobmi, avšak na spoločnom princípe odlíšenia skupín používateľov s rozlične definovanými právomocami. Napríklad v rámci navrhovanej WMS je možné vytvoriť skupiny používateľov:

– *verejnosť*, používatelia tejto skupiny smú len prehliadať nami poskytované geodáta,
– *zamestnanci*, tejto skupine je, okrem prehliadania, umožnená aj práca s geodátami, tvorenie, editovanie a mazanie,
– *administrátor*, úzka skupina administrátorov má okrem možností prvých dvoch typov právomoc prevádzkovať server, definovať práva ostatných členov a pod.

Vrstvenie je v každom type softvéru riešené iným spôsobom. Databázový systém Oracle umožňuje definovať skupiny práv, tzv. role, ktoré zjednodušujú proces definície prístupových práv jednotlivým používateľom. Databázový systém PostgreSQL toto zjednodušenie rieši vytvorením skupiny používateľov a následne definíciou právomocí hromadne v rámci skupín. Ak na vytvorenie WMS použijeme ArcGIS Server, podľa typu pripojenia máme možnosť rozhodnúť sa medzi definovaním používateľských skupín (miestna sieť), alebo rolí obnášajúcich dané právomoci, spojených s konkrétnou WMS (internet).

V rámci zachovania bezpečnosti, v zmysle prevencie úniku dôležitých informácií, je výhodné taktiež rozvrstvenie možnosti prehliadania geodát. Zahŕňa definovanie mierky alebo rozlíšenia mapy, ktoré sú ešte prístupné na prehliadanie všetkým používateľom, a na prehliadanie ktorých je potrebné prihlásiť sa používateľským menom a heslom. Toto opatrenie môže byť užitočné pri publikovaní geodát, ktoré obsahujú citlivé informácie, napr. o lokalizácii archeologických alebo iných nálezísk, vojenských objektov a podobných lokalít.

Záver

Podcenením bezpečnosti dát v akomkoľvek štádiu práce s nimi môže dôjsť k škodám nielen úmerným k cene dát, ale aj k takým, ktoré ich pôvodnú cenu niekoľkonásobne prevyšujú. Preto je treba poznať riziká, ktorým sú dáta vystavené, možnosti, ako tieto riziká čo najviac eliminovať a zároveň posúdiť, ktoré riešenie je najvhodnejšie a najefektívnejšie s ohľadom na cenu a hodnotu dát, ktorá je pri geodátach značná, vzhľadom na náročnosť ich získavania, spracovania a ich výpovednú hodnotu. K bezpečnosti dát inak pristupuje používateľ a inak prevádzkovateľ servera a neraz je nutná konzultácia s odborníkom na inú časť procesu práce s dátami.

Literatúra

ENDORF, C., SCHULTZ, E., MELLANDER, J. (2005). *Detekce a prevence počítačového útoku*. Praha (Grada Publishing, a. s.).

MATIAŠKO, K. et al. (2008). *Databázové systémy. Základy databázových systémov*. Žilina (EDIS – vydavateľstvo Žilinskej univerzity).

MATIAŠKO, K. et al. (2004). *Základy informatiky*. Žilina (EDIS – vydavateľstvo Žilinskej univerzity).

OGC® Standards and Specifications. [cit. 2010-04-27] Dostupné na: <http://www.opengeospatial.org/standards>

S u m m a r y

Security of online data publishing

The purpose of this thesis is to summarize risks of publishing geodata.

OSI reference model (Open System Interconnection Reference Model) is the background of network processes. It consists of seven layers (Endorf et al., 2005) with specific roles, but in general each layer complements a layer immediately below, and also forms the basis for the functionality of the layer immediately above. Functionality and security of the system for publishing data depends on impeccable follow-up of layers, but also on recognition of risks, that are different for each layer. It is necessary to recognize the vulnerabilities of the system and to consider the costs necessary to prevent threats in way, which is effective and adequate to value of data.

Safety of the system is guaranteed by (Matiaško et al., 2004) privacy, integrity, availability and authenticity. Privacy may be guaranteed by applying measures against the unauthorized viewing of data. This may be software, but also rules for minimizing the damages caused by human error.

Data integrity ensures the accuracy and sureness of data content. Functionality of the system and its protection against malware reduce risk of unauthorized data modifications. Malware means program for the marauding activities of infected computers. Firewall and antivirus software is used against these threats, but also prevention is important (not to open emails from suspicious senders, advertising or other suspicious web sites).

Data availability ensures authorized access to data. System capacity should be sufficient to avoid collapse, the loss or damage data. There are few measures against data loss, for example backup, using backup equipment during power system and competent crew for case of re-entry into service.

Data authenticity guarantees their origin and content. Electronic signatures are sometimes used to confirm authenticity.

Interface, which is formed by standardized protocols of OpenGIS Consortium (OGC), allows clients to access the map server, where data are stored. Maps of spatial data are generated on the basis of geographic information, which is awarded by client. Maps can be delivered as raster image or in vector format by web map services (WMS). If the service delivers geodata itself, it is called Web Feature Service (WFS).

The risks, mentioned in the previous parts of thesis, threatening data in general, include also unauthorized access. The prevention can be solved in multiple ways, but all the solutions include principle of distinction of differently defined users' privileges (access, data editing, view, loading). Stratification of browsing geodata is also useful as prevention of lost of important information about position of objects as archaeological sites or army objects.

Recenzovali:

Ing. Jana FAIXOVÁ CHALACHANOVÁ, PhD.,
Ing. Tibor LIESKOVSKÝ, PhD.,
Slovenská technická univerzita, Stavebná fakulta,
Bratislava