Bezpečný web

Každý třetí český IIS Web je děravý

Když v červenci spatřila světlo světa služba URLcheck, zdaleka to nevypadalo tak černě. Ovšem v okamžiku, kdy pomocí tzv. Translate:f chyby došlo k úspěšnému napadení serverů reklamní služby Mr.Linx, bylo už vcelku jasné proč. URLcheck, extrémně jednoduchá služba, umožňující ověřit úroveň zabezpečení proti nejčastějším bezpečnostním chybám, ukazovala na velký problém. V polovině srpna již každý třetí testovaný web byl děravý, kdokoliv s prohlížečem se mohl dostat ke zdrojovým kódům ASP stránek.

Provozovat počítač připojený k internetu, ať již jako WWW server či jakýkoliv jiný server, je věc mimořádně ošemetná. Každý se totiž může připojit. A každý může zkoušet, kde tesař nechal díru. A čím známější webové stránky provozujete, tím více je těch, kdo zkoušejí proniknout dovnitř. Den co den je na světě napadeno několik desítek webů (a pravděpodobně dalších několik desítek zůstane nepovšimnuto, neb nestojí za pozornost ani médií, ani těch, co sbírají úspěšně napadené stránky).

Úměrně rozšíření webů provozovaných na platformě Microsoft IIS (Internet Information Server) se množí útoky právě na tyto weby. A nutno zdůraznit, že v mnoha případech to mají hackeři velmi, velmi snadné.

Řada správců a provozovatelů strojů s Windows NT/2000 totiž zcela zoufale zanedbává ta nejzákladnější pravidla vedoucí k provozu bezpečného WWW. Možná by se i dalo říct, že jim chybí to, co většina unixových či linuxových administrátorů nepostrádá – dobré znalosti o tom, co provozují a spravují. Provoz webového serveru totiž není o tom, jak rychle někdo zvládl klepání myší za účelem založení virtuálního adresáře, ale o pochopení všech souvislostí a o vysoké úrovni znalostí.

Snad trochu pomůže projít ve stručnosti nejčastější nebezpečí vyskytující se na webech okolo nás a v mnoha případech také vedoucí k hacknutí, ztrátě dat, integrity atd. Jak ale nakonec sami zjistíte, největším nebezpečím pro webový server je ve skutečnosti jeho správce.

Sdílený prostředek

Snem každého hackera začátečníka je web nabízející na své IP adrese také sdílený prostředek. Nejlépe rovnou disk, kde jsou uložena data webu a kde jsou uložena, aniž by byla jakkoliv omezena, přístupová práva. Hacker začátečník pak napíše NET USE H: web.co.chci.hacknout.cz\\diskc a pak už jenom používá příkazy COPY a DEL.

Připadá vám to absurdní? Kdepak, před několika týdny byl hacknut web jednoho pražského deníku. Jak? Snadno. Jeho administrátor nechal disk sdílený právě popsaným způsobem.

Přístupová práva

Práva jsou od toho, aby byla přidělována a ubírána. Nic horšího nemůže potkat správce webu, než že na něco takového zapomene a přidělí práva například skupině EVERYONE pro sdílený prostředek či ponechá možnost informací upload přes HTTP a zapomene zamezit zápisu do webových adresářů.

A vůbec nejhorší jsou lidé, kteří nainstalují web na Windows 95/98 či na Windows NT 4.0 a použijí disky FAT. Zde se totiž žádná přístupová práva nastavovat nedají. Pro hackery začátečníky úplně ideální.

Frontpage Server Extensions

Nejoblíbenější nástroj hackera pokušitele je Microsoft FrontPage. Prostě namíří na některý web a zkusí jej otevřít. A tak v jednom z dvaceti případů s překvapením zjistí, že se mu web otevřel a že na něm může dělat úplně cokoliv. Administrátor totiž patří mezi zvláštní sortu lidí, co buď nečtou dokumentaci, nebo nevědí, co dělají – a tak nechávají web otevřený přes FrontPage pro skupiny jako EVERYONE. Či pro jistotu nenastavují omezení vůbec.

Opět vám to připadá absurdní? Ale kdepak. Čerstvé příklady z poslední doby zahrnují jednoho vydavatele celostátních týdeníků a měsíčníků. A abychom nebyli jenom u českých prohřešků, také jednoho výrobce velmi dobrých PDA. V posledním jmenovaném případě pomohl až ostrý dopis jeho tiskovému mluvčímu; webový administrátor si totiž asi myslel, že si z něj dělám legraci. Asi by tehdy bývalo rychlejší mu to hacknout.

Mimochodem, aby to nevypadalo, že za to vlastně mohou FrontPage Server Extensions. Stejný problém můžete napáchat s FTP serverem (a může to být klidně Unix). Pokud někde necháte otevřené dveře, hacker je dříve či později vždycky najde.

Přístupová hesla

Další příklad absurdností je v kategorii přístupových hesel. Praktický příklad starý také pár týdnů. Web bylo možno hacknout snadno, uživatel TEST měl heslo TEST a ještě navíc byl ve skupině Administrators. Netřeba snad zdůrazňovat, že v tomto případě bylo možné kompletně ovládat celý stroj Windows NT pomocí nástrojů na dálkovou správu. Po upozornění na problém byl odpovědí pouze sprostý dopis.

Poučení? Pro stroj připojený k internetu platí daleko přísnější pravidla pro vytváření a údržbu hesel. Heslo musí být složité (vždyť není nic složitého postupně několik dní zkoušet podle slovníku nebo podle kombinací) a neodhadnutelné. A co víc, musí se často měnit.

Mezi ukázkové příklady spadající do této kategorie patří weby, kde uživatelé nemají žádná hesla. Zcela pravidelně se toto navíc stává u instalací SQL serveru – uživatel “sa” bez hesla je sice další absurditou, zato vcelku pravidelně se objevující.

Zdrojové kódy ASP

Je až s podivem, kolik škody mohou způsobit bezpečnostní chyby umožňující získat přístup ke zdrojovým kódům souborů ASP a ASA. Ve většině případů se totiž právě v nich najdou další zajímavé údaje – umístění databází Access (je až nepochopitelné, kolik naivních tvůrců webů umisťuje databáze Access do míst volně přístupných pomocí prohlížeče) a zejména hesla do SQL serveru. Úplně nejhorší kombinací, která se podepsala na již zmiňovaném hacku Mr.Linxe, je použití “sa” účtu (administrátor SQL) pro přístup k databázím z ASP stránek.

Hacker mírně pokročilý tak získá přístup k SQL serveru, pomocí příslušné uložené procedury spustí příkaz pro změnu hesla účtu Administrator a cestu ke stroji má kompletně otevřenou. A samozřejmě má i přístup ke všem údajům v databázích.

Mezi chronicky zneužívané bezpečnostní chyby tohoto druhu patří tzv. NULL.HTW, +.HTW, Translate:f, $DATA a CodeBrws.ASP – všechny mají něco společného. Jednak umožní přístup ke zdrojovým kódům, jednak byly již dávno opraveny a nikdo by jimi neměl trpět. Přesto každý třetí web testovaný na URLcheck (viz svet.namodro.cz/urlcheck.asp) vykazuje děravost na některou z těchto chyb. A pokud jste si ještě neotestovali ten svůj web (nemusíte jej fyzicky provozovat, čeští ISP jsou nepoučitelní tak jako tak), měli byste to rychle udělat. Na stránkách URLcheck najdete i kompletní návody, jak se všech jmenovaných chyb zbavit.

Přístup k administraci webu

Pokud si myslíte, že jenom šílenec by mohl nechat administrační část webu či webové aplikace volně přístupné veřejnosti, pravděpodobně se mýlíte. Weby s volně přístupnými aplikacemi IISADMIN či IISADMPWD jsou zcela běžné. A ještě běžnější jsou webové aplikace, které nekontrolují přihlášení do administrační části aplikace. Jejich tvůrci se totiž zpravidla spoléhají na to, že nikdo “neví”, kde se příslušná administrační URL nachází (nemají ale dostatek nápadů, takže se většinou jmenují /ADMIN, /ADM či jakkoliv smysluplně). Případně naprogramují přihlašování, které ověřuje přístup pouze k první stránce a další ponechají zcela volné.

Neošetřené vstupy

Neošetření údajů vstupujících od uživatelů webu patří paradoxně k velmi častému způsobu hacků webu. A dokonce stejně často ve windowsovém i unixovém prostředí. Zpravidla je totiž parametr skriptované stránky použit jako parametr předaný nějakému skriptovacímu jazyku, ať již jde o SQL dotazy či vykonání příkazů operačního systému. Pak už stačí jenom málo: vědět, co je “za tím”, a vsunout modifikovaná vstupní data. Tudy paradoxně často vede cesta do SQL serveru (a následně k operačnímu systému) či přímo k vykonání nějakých těch užitečných příkazů operačního systému.

Mezi neošetřené vstupy ovšem patří i řada “buffer” či “stack overflow”. Zde je většinou vina na tvůrci operačního systému či aplikace. V případě Windows jsou tyto chyby zneužitelné většinou jenom k havárii stroje, v případě programů Unix/Linux jsou ovšem zdrojem hacků ve většině případů.

Přístup k registru

Přístup k Registry (hierarchická databáze udržující informaci o konfiguraci Windows o/s a programů) je také častým zdrojem hacků. Bohužel pro provozovatele nevěnoval Microsoft zpočátku příliš pozornosti zabezpečení některých klíčů. Je tak možné například snadno podvrhnout některé programy, které se spustí při příštím restartu počítače či přihlášení uživatele. Zkušený hacker tak musí jenom chvíli počkat a pak sklidit plody svého úsilí.

Ale i zde existuje ochrana. Spočívá v nastavení "správnějších" přístupových práv a pochopitelně ve znepřístupnění Registry z počítačů, které k tomu nemají mít nárok.

Fulltextové vyhledávání

Fulltextové vyhledávání je dobrý sluha, ale také špatný pán. Je až s podivem, kolikrát se do fulltextového katalogu dostanou dokumenty, které tam nemají co dělat. S pomocí Altavisty je tak možné najít tisíce děravých webů, stačí znát tu správnou část URL s bezpečnostní dírou a nechat si ji vyhledat. Stejně tak je známo několik bezpečnostních děr, které umožňují zneužít právě fulltextové vyhledávání pro přístup ke zdrojovým kódům souborů ASP/ASA.

Ignorování dění

Zde nejde o přímou bezpečnostní chybu, ale o prostou nevšímavost. Každý operační systém a prostředí nabízí řadu příležitostí ke sledování dění. Podezřelé dotazy je možné zaznamenávat, chronicky známé věci je možné "odvádět" jinam (či klidně vzbuzovat falešné zdání). Nepřípustnou komunikaci na nevhodných portech je možné filtrovat. Změny souborů a účtu je též možné monitorovat. Ve většině případů si vystačíte s tím, co již máte, a nebudete muset nic dokupovat. Pokud máte dostatek prostředků, existuje řada programů schopných vykonávat audit v reálném čase a neprodleně varovat. Tyto prostředky navíc mají k dispozici neustále aktualizovanou databázi problémů a můžete tak skutečně předejít řadě nepravostí (antivirové programy už také přece používáte zcela rutinně).

Dostupná je i řada prostředků na jednorázové vykonání bezpečnostní kontroly. Řada z nich je zadarmo (a zvládá většinou přesně to, co potřebujete), mnohé další je možné koupit se zárukou profesionality a aktuálnosti. Podobné prostředky by měly patřit k základní výbavě všech ISP/IAP/ASP, ale skutečnost je většinou dosti zoufalá.

Jasně že to není všechno!

Samozřejmě, výše uvedené je jenom slabým zlomkem toho, co byste měli dělat pro zabezpečení svého webu. Chip nemá k dispozici neomezený počet stránek, ale internet naštěstí ano. Za čtyři roky věnování se tomuto "odvětví" informačních technologií nashromáždil Svět Namodro tisíce článků právě o bezpečnosti – najdete je na security.namodro.cz včetně odkazů na řadu důležitých zahraničních zdrojů. Samozřejmě se zaměřují hlavně na technologie Microsoftu, takže pokud vás oslovuje Linux či Unix, mohu doporučit www.root.cz či www.underground.cz – věnují se tam Linuxu a Unixu z hlediska bezpečnosti minimálně stejně dobře.

Daniel Dočekal