Bezpečnost hostovaných aplikací

Zdeněk Brůna

Hostování aplikací znamená zajistit zákazníkům takovou míru bezpečnosti, aby byli ochotni svěřit svoje data do rukou cizího subjektu. Jaká konkrétní bezpečnostní opatření můžete u hostingových poskytovatelů v ČR očekávat, jaká ne a proč? Jak vnímají bezpečnostní opatření zákazníci, jak moc je pro ně bezpečnost důležitá? Co všechno si lze pod pojmem bezpečnost v případě hostingu představit?

Co vše hoster ohledně bezpečnosti řeší?

Dovolím si nejdříve velmi stručně projít všemi důležitými oblastmi, které nemohu v článku o bezpečnosti hostovaných aplikací vynechat.

Bezpečnost a utajení dat

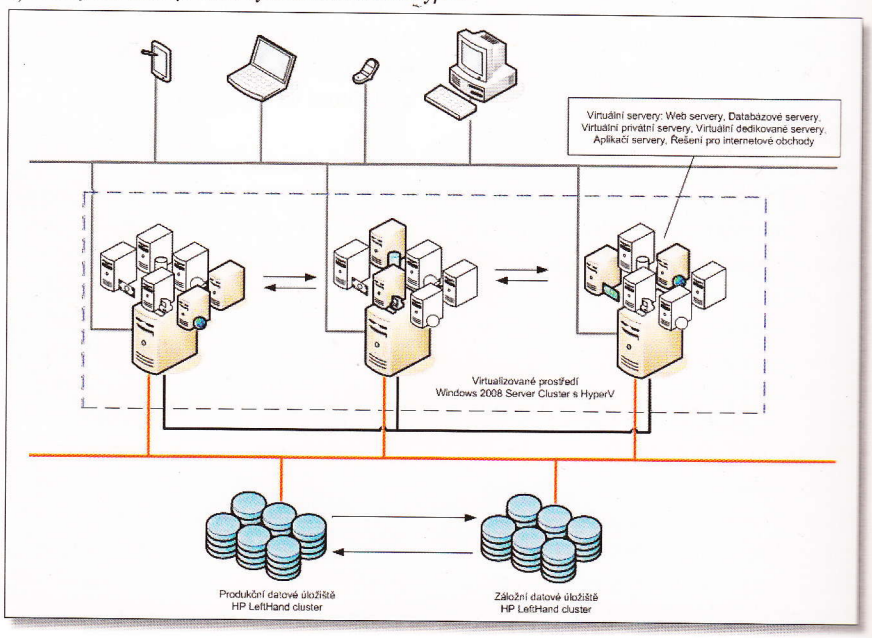
Fyzickou bezpečností serverů, datového centra je nutné začít. Poskytovatel služby musí zajistit, aby se k jeho zařízení nemohl dostat nikdo nepovolaný. A ty povolané musí velmi pečlivě vybírat a mít kontrolu nad tím, jak svých přístupů využívají. Proto má odpovědný hoster svoje servery umístěny ve špičkovém datacentru a jeho administrátoři jsou zkušení profesionálové s vysokou mírou odpovědnosti. Hostingový provider má totiž veškerý svůj byznys postavený na důvěře od svého zákazníka, jakákoli ztráta důvěry může v důsledku znamenat vážné ohrožení jeho existence. Proto je bezpečnost denním chlebem každého kvalitního hostera.

S bezpečností dat souvisí i jejich vysoká dostupnost. K čemu jsou zákazníkovi zabezpečená data, pokud mu nejsou v požadovaný okamžik dispozici? Proto bych zákazníkovi doporučil vybírat takové poskytovatele hostingu, kteří mají alespoň dvě fyzicky odlehlá datová centra, která disponují vždy nejméně dvěma nezávislými připojeními do Internetu. Hostery, jejichž infrastruktura je zdvojená a pracuje ve failover režimu. Špičkovými datovými centry se myslí ta, která poskytují definované parametry prostředí (teplota, vlhkost, bezprašnost), vysokou redundanci pro napájení a chlazení serverů, automatický protipožární systém a jsou umístěna mimo záplavovou oblast.

Další důležitou záležitostí, kterou hoster musí řešit, je segregace dat, tj. jejich oddělení pro jednotlivé zákazníky. Nejnáročnější klientele lze nabídnout provoz řešení na serverech určených pouze pro jednoho zákazníka, provoz v nezávislé VLAN, poskytnutí VPN, zabezpečení vlastním firewallem a celou řadu dalších opatření šitých přímo na míru potřeb konkrétního zákazníka. Drtivá většina klientů hostingu obecně však využívá sdílených prostředků, protože je to výrazně levnější a přemíra bezpečnostních prvků je mnohdy pro tyto zákazníky nepřijatelná. Zvyšuje složitost řešení a mnohdy i obsluhu pro koncového uživatele. I zde je však možné potřebnou segregaci zajistit, většinou nastavováním uživatelských práv pro jednotlivé uživatele a jimi využívané adresáře, pomocí aplikačního poolu nebo nastavením interpreteru skriptů. Každý z hosterů považuje tato nastavení za své cenné know-how, jehož hodnota se zvyšuje s délkou zkušeností poskytovatele a počtem obsluhovaných zákazníků.

Poslední problematikou, kterou v tomto ohledu zmíním, je šifrování a přenos dat. Přínosy šifrování dat jsou pro drtivou většinu hostingových zákazníků poměrně malé a příliš často se k němu nepřistupuje. Zašifrováním dat se totiž obecně zhoršuje jejich dostupnost a výrazně snižuje schopnost hostera plně obnovit provoz aplikace v případě výpadku. Naprostou nutností je však nabídnout zákazníkovi šifrování přenosů dat, protože k nim přistupuje výhradně přes internet. Základem pro to je rozhodně podpora SSL, a to v lepším případě při využití komerčních certifikátů, kde je kromě šifrování umožněna i autentizace komunikujících stran. Od SSL je již jen krůček k HTTPS, tedy k internetovému brouzdání bez možnosti odposlechu komunikace mezi návštěvníkem stránek a webovým serverem. Nebo k FTPS (případně SSH), kdy má klient možnost umísťovat aktualizace svých webových prezentací na webový server zabezpečenou formou. Dalším příkladem, který zde uvedu, je IMAPS, kdy klientovi umožňujeme šifrovanou komunikaci s mailovým serverem. Důležitým se vzhledem ke stále rozšířenějšímu provozování aplikací formou SaaS stává také RDP over SSL.

Řešení vysoké dostupnosti s využitím Microsoft HyperV



Dodržování standardů BCM, smluvní podmínky, legislativa

V době, kdy se z ekonomických důvodů provozuje z prostředí hostingu nebo i cloudu stále více a stále důležitějších služeb je nutné věnovat se i otázce business continuity managementu, tj. zajištění kontinuity běhu klíčových procesů společnosti na stanovené úrovni i v případě technické nebo administrativní chyby poskytovatele hostingových služeb, která může vždy nastat.

Proto důrazně doporučuji, aby si každý zákazník, pokud plánuje hostovat své byznys aplikace (ať už se jedná o e-maily, webové stránky, ekonomické aplikace nebo jiné služby), důkladně prostudoval smluvní dokumenty (VOP případně smlouvu), tj. garance, jaké poskytovatel hostingu nabízí, a zda jsou smluvní podmínky v souladu s platnou legislativou. V kombinaci s informacemi o stabilitě a renomé hostera (doba působení na trhu, ekonomické výsledky, podpora nových technologií, obecné povědomí o firmě) to pak dává odpovědné osobě zákazníka potřebné informace k učinění správného rozhodnutí, komu svěří do péče svoje data nebo aplikace, o koho opře svůj byznys, komu zaplatí za předplatné služeb.

Ano, získat všechny tyto informace je obtížné, ale po více jak sedmiletém působení v oblasti hostingu mohu zodpovědně říci, že se toto pátrání vyplatí. Již několikrát jsem se osobně setkal se zákazníky, kteří se ocitli v existenčních obtížích, když tuto fázi výběru hostera podcenili. Jejich hoster je posléze „odměnil" náhlým snížením kvality služeb a mnohdy zároveň s tím i neférovostí při jednání. Byl jsem tak například svědkem obrovské frustrace a stresu našeho bývalého zákazníka, který od nás před lety odešel za levnější konkurencí. Tento zákazník osobně přišel, v ruce držel svůj mailserver a se slovy, že jeho hoster odjel na dovolenou a že mu již tři dny nefungují firemní e-maily, prosil o pomoc. Kromě několikadenní nefunkčnosti svých e-mailů a nevymahatelnému předplatnému zákazník nakonec zjistil, že celou dobu platil svému dodavateli za službu, která mu nebyla ve skutečnosti nikdy poskytována. Na server jsme se navíc přihlásili pod heslem, které dostal zákazník na předávacím protokolu při svém odchodu od nás a poslední, kdo se kdy k serveru přihlásil pod root accessem jsme byli právě my před lety! Server tak nebyl několik let vůbec updatován a byl plný závažných bezpečnostních děr!

Jaké aplikace hoster typicky zabezpečuje?

V případě hostera jsou aplikace programy, které jsou nainstalovány na servery, využívají služeb operačního systému a pomáhají zákazníkům při jejich práci nebo jim slouží k zábavě. Prostor pro tento článek je příliš malý na jejich úplný seznam, proto se dále zmíním jen o několika nejdůležitějších aplikacích, které hoster musí zabezpečovat. Nemohu ale opomenout ani služby, které jsou pro ně nezbytným doplňkem, byť to třeba nejsou aplikace v pravém slova smyslu. Poskytovaná služba je totiž tak bezpečná, jak je bezpečný její nejslabší článek.

Systémem DNS vše začíná i končí...

Začnu u systému DNS, jehož překlad adres z lidské do počítačové řeči je základem pro všechny další hostované služby, aplikace. Všichni totiž systém DNS využíváme, aniž to mnohdy víme. Důležitost zabezpečení tohoto systému uvedu na příkladu. Každý z vás zřejmě obdržel e-mail, ve kterém bylo někdy šikovněji, někdy méně šikovně napsáno, že v rámci dalšího fungování nebo bezpečnosti vaší služby (e-mailu nebo internetového bankovnictví) je nezbytně nutné, abyste se okamžitě přihlásili do systému a řídili se tam dalšími pokyny. V e-mailu byl odkaz, který navenek vypadal důvěryhodně (obsahoval jméno vám důvěrně známé služby), a pokud jste na něj klikli, otevřel se vám browser s přihlašovacím oknem. Naštěstí si drtivá většina z vás všimla, že v adresním řádku prohlížeče již není adresa vaší hostované aplikace, ale adresa zcela jiná. Údaje do přihlašovacího okna jste tak nezadali i přes to, že použitá grafika na webových stránkách byla velmi podobná té, kterou využívá pravý poskytovatel služby. Potkali jste se s tzv. phishingem. Co se ale stane, pokud bude v adresním řádku odkaz zcela v pořádku, přesto bude směřovat na falešné servery útočníka, tedy pokud se potkáte s tzv. pharmingem? Daleko více z vás svoje jméno a heslo zadá a bude spoléhat na to, že systém DNS vám podstrčenou adresu přeloží na správnou IP adresu a vaše cenné údaje pošle opravdu do banky nebo provozovateli webmailu. Chyba! Systém DNS v sobě žádné takové ochranné mechanismy nemá a pokud váš poskytovatel připojení do internetu a provozovatel autoritativního nameserveru k doméně (velmi často registrátor) nepodporuje DNSSEC, tedy zabezpečenou verzi DNS, pak velmi riskujete. Technologie DNSSEC totiž snižuje například rizika:

- zneužití vašich e-mailových schránek,
- prozrazení choulostivých dat (přístupová hesla, údaje o platebních kartách atd.),
- útoku na obsah vaší webové prezentace.

DNSSEC tedy zcela jistě zasluhuje, aby byl vašimi internetovými providery podporován, ptejte se po něm. V současné době totiž registrátoři zabezpečují necelou jednu šestinu domén CZ a situace s jeho podporou u ISP bude zřejmě ještě daleko horší.

A co hostované e-maily?

Zdánlivě banální služba, kterou mnozí z nás používáme více než deset let. A právě pro svoji rozšířenost je e-mail snad nejčastějším terčem útoků nejrůznějších zájmových skupin. Ať už to jsou spameři, kteří nás obtěžují svými nabídkami na prodloužení čehokoliv, nebo závažnějšími trestními činnostmi, jako je například šíření dětské pornografie. Dalším příkladem mohou být phisheři a pharmeři, kteří e-maily používají pro rozesílání podvodných odkazů, jež jsem zmiňoval ve svém příkladu výše. Nemůžu zapomenout na zneužití e-mailů pro rozesílán virů, které následně od koncových uživatelů získají přihlašovací údaje nebo jiná cenná data, případně z jejich počítačů udělají zombie a ty pak slouží k dalšímu šíření nákazy. V každém z uvedených případů nemusí poskytovatel hostovaného e-mailu dělat nic a nechá veškerou odpovědnost za boj s těmito živly na koncovém uživateli služby, nebo se snaží maximálně pomoci. Odpovědní poskytovatelé pak neustále rozvíjejí ochranu mailboxů svých zákazníků pomocí antiviru a antispamu, kterou dále doplňují o sofistikované nástroje, jako jsou greylisting nebo DKIM.

Greylisting využívá faktu, že spameři obvykle neodesílají e-maily opakovaně, pokud je poprvé příchozím mailserverem odmítnut. Tímto způsobem dojde k odmítnutí více než 95 procent spamu.

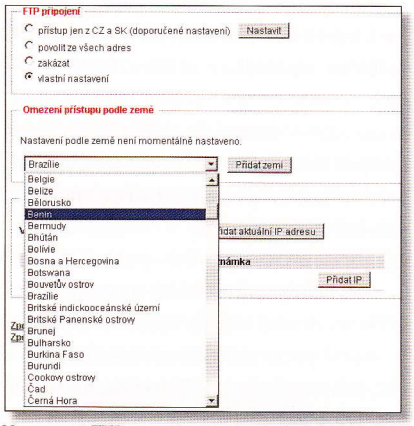
DKIM pak za pomocí asymetrického šifrování dokáže zaručeným způsobem ověřovat, že konkrétní e-mail (včetně jeho nezměněného obsahu) byl zaslán z nějaké domény. Bez využívání DKIM je možné adresu odesílatele u e-mailů libovolně falšovat. S DKIM můžete ověřit, že odesílatelova doména falešná není. Při použití DKIM poznáte, že byl e-mail odeslán skutečně z domény pisatele e-mailu a také že obsah e-mailu nebyl cestou nijak modifikován.

Webhosting a webové aplikace

O segregaci a šifrování přenosu dat, které jsou základem i pro webhosting, jsem psal výše a jsou to záležitosti obecně známé a používané. U webhostingu a hostování webových aplikací však hoster naráží na jeden zásadní problém. Veškerá zabezpečení, která jsou ze strany hostera provedena, mohou přijít vniveč, pokud se rovněž zákazník nechová

zodpovědně. Mám tu dva příklady, se kterými se velmi často setkáváme.

Zákazníci neupdatují své FTP klienty (proč taky, když neupdatují ani svá PC), nechávají v nich uložené přístupové údaje ke svým webovým stránkám v plain textu a nabízejí je tak na zlatém podnosu hackerům. Tito většinou plně automatizovaně a velmi rychle takové přístupy získají a pomocí nich na web umístí obsah, jaký se jim zlíbí. A to velmi často takový, který poškozuje dobré jméno vlastníka webových stránek, a v horším případě mu může přivodit i trestní stíhání (například v případě umístění dětské pornografie nebo stránek pomáhajících phisherům nebo pharmerům). Snahou každého hostera je proto vzdělávat své zákazníky tak, aby se ke svým účtům chovali zodpovědně, ale to se nikdy nemůže zcela podařit. Pro zlepšení situace ohledně zcizených FTP účtů jsme proto v naší společnosti přistoupili k vyvinutí vlastní FTP autorizace, která omezuje možnosti přístupu na webové servery pomocí FTP podle IP adresy nebo lokality. Incidenty tohoto typu se tímto způsobem podařilo téměř zcela eliminovat.



Nastavení FTP autoriazace v administračním rozhraní

Mnoho zákazníků si svoji webovou aplikaci vyvíjí amatérsky svépomocí nebo používají „prefabrikáty" ve formě různých CMS, které pak ale neaktualizují, když jsou v nich odhaleny chyby. Proto hoster musí bezpečnost aplikací řešit do značné míry za zákazníka na jiných úrovních (konfigurace serveru, preventivní sledování podezřelých změn, reagování na známé chyby v rozšířených CMS apod.). Všechna opatření je ale nutno provádět rozumně s ohledem na funkčnost aplikací zákazníka, která nesmí být omezena a zákazníkovi by měla zůstat svoboda tato opatření vypnout. Aktuálním příkladem z poslední doby je masové zneužívání chyby v open source aplikaci OsCommerce/ZenCart. V Active 24 jsme byli nuceni nasadit do provozu automatizovanou změnu konfigurace PHP pro všechny webhostingy, které tuto aplikaci využívají. Zabránili jsme tak zneužití této chyby a přitom negativně neovlivnili fungování aplikace pro zákazníka.

Aplikační servery

V loňském roce jsme spustili novou službu Aplikační servery, které jsou postaveny na distribučním modelu SaaS. Zákazníkovi jsou nabízeny aplikace jako Pohoda, Abra nebo Money a jeho koncoví uživatelé k nim přistupují pomocí RDP over SSL. Zabezpečili jsme tak přenosy dat mezi serverem a uživatelem. Zároveň jsme uživateli zachovali veškerý komfort při spouštění aplikace, protože jsme mu díky Terminal Server Remote Applications mohli na jeho pracovní plochu umístit ikonu aplikace, a on ji tedy spouští tak, jako kdyby ji měl nainstalovánu lokálně.

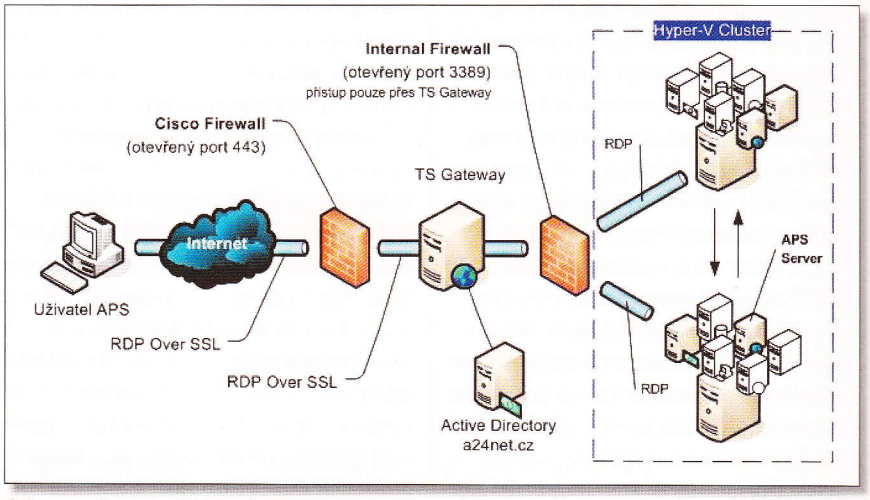


Schéma zabezpečení služby Aplikačních serverů

Při uvedení služby jsme přesto narazili na další bezpečnostní specifika této služby. Tím prvním byla otázka, zda je v pořádku, aby byla ekonomická data, tedy data velmi citlivá, umístěna v prostředí hostingu, zda je to bezpečné. Odpovědět si zákazník dokázal většinou sám. Když jsme s ním totiž začali probírat, jak se nyní stará o zabezpečení serveru s aplikací, tak na celou řadu našich otázek neznal odpověď, nebo odpovídal, že to buď vůbec neřeší, nebo se o to stará jeho administrátor, vývojář a IT support v jedné osobě. Zákazník tak velmi rychle pochopil, že pro bezpečnost svých dat nyní nedělá a ani nechce dělat ani zlomek toho, co nabízíme my jako poskytovatel hostingu. Ušetřený čas prý bude radši věnovat rozvoji svého podnikání. Nakonec jeho důvěra v náš subjekt je již léta prověřena poskytováním e-mailových služeb a webhostingu.

Druhou otázkou, kterou jsme od našich zákazníků slyšeli, byla, zda jim umístěním ekonomických dat u nás neroste riziko toho, že se k těmto datům dostanou rychleji například úředníci finančního úřadu při kontrole hospodaření firmy. Neodpovídalo se mi na tuto otázku lehce, ale pravda je taková, že pokud firma nemá co skrývat, pak toto řešit nemusí. Poskytovatel hostingu je povinen data vydat, pokud k tomu dostane příkaz od soudu či policie, přesně v souladu se zákony. Data však musí zákazník vydat i v případě, že je má u sebe v kanceláři. V tomto ohledu se pro zákazníka opravdu nic nemění.

Přesto jsme však u Aplikačních serverů začali uvažovat o šifrování filesystému využitím TrueCrypt. Chtěli jsme nabídnout variantu, aby nebyla ani pro nás jako provozovatele hostingu data nijak čitelná. Prozatím však tuto možnost nikdo nepoptával. Zřejmě proto, že zároveň znamená nemožnost využití TS Remote Application, snižuje naše možnosti při obnově běhu aplikace po závadě na serveru, a ještě navyšuje cenu řešení, protože šifrování znamená vyšší čerpání námi poskytovaných systémových prostředků. Narážíme opět na to, že klient není ochoten vyměnit vyšší bezpečnost za snížený komfort obsluhy a vyšší cenu.

Závěrem

Řešení bezpečnosti z hosterovy strany je ale vždy potřeba dělat rozumně s ohledem na funkčnost hostovaných aplikací, která nesmí být opatřeními omezena, a zákazníkovi by měla zůstat možnost bezpečnostní opatření nevyužívat. Hoster tedy musí v tomto ohledu hledat rozumnou rovnováhu, a zejména nemůže omezovat zodpovědné zákazníky s bezpečnými aplikacemi kvůli těm, kteří na bezpečnost nedbají. Hledání tohoto kompromisu je obtížná disciplína, kterou se velmi často od sebe jednotliví poskytovatelé hostingu odlišují daleko výrazněji než rozdílem cen za poskytování služeb. ■

Autor je technickým ředitelem společnosti Active 24.