Technický popis Server TimeMaker

Použité technologie

Frontend – Klient TimeMaker (Deplhi), IE 6.0,
Backend – Aplikační server (Java), databáze MySQL/PostgresQL/Oracle,
Operační systém – GNU/Linux – Doporučujeme CentOS, podporováno je také Ubuntu, Debian, RHEL, SUSE a další standardní serverové distribuce.

Zabezpečení systému TimeMaker

Zkratky a pojmy

TimeMaker (TM) – komunikační systém
Aplikační server (AS) – stroj, na kterém je provozován systém TM
Lokální přístup (LP) – získání přístupu k serveru probíhá pouze fyzicky za pomocí klávesnice a monitoru
Vzdálený přístup (VP) – možnost získání přístupu k serveru ze vzdáleného místa, které je propojeno se serverem pomocí Internetu
Linux – pojmenování operačního systému
SSH – zabezpečený a šifrovaný přístup k aplikačnímu serveru
HTTPS – zabezpečený a šifrovaný transportní protokol mezi serverem a internetovým prohlížečem
Administrátor – osoba disponující oprávněním ke správě serveru, IS, atd.
PHP – programovací jazyk
Firewall – zařízení, které chrání počítače umístěné za firewallem před útoky (Hackerů – nežádoucí osoba) a neoprávněnými přístupy ze sítě
IP adresa – jedinečná číselná adresa v rámci dané sítě (např. Internet, lokální síť)

Bezpečnostní opatření systému TM se v zásadě dělí do dvou skupin:

- **Vnější ochrana** – bezpečnostní opatření zabraňující průniku do systému z venku. Např. zabezpečení serveru, zabezpečení databáze, fyzické zabezpečení serveru,
- **Vnitřní ochrana** – bezpečnostní opatření zabraňující průniku do systému zevnitř. Např. definované úrovně uživatelského přístupu, systém práv.

Vnější ochrana systému

Fyzická ochrana aplikačního serveru

Server je umístěn v uzamčené technologické skříni v klimatizované místnosti (serverovna), do které je možný přístup pouze na základě dokladů totožnosti a seznamu oprávněných osob. Objekt, ve kterém se nachází serverovna, je pod non-stop dohledem bezpečnostní agentury.

Oddělení od sítě Internet

Aplikační server je umístěn za firewallem, který filtruje veškerý přenos mezi serverem a Internetem. Tento firewall dovoluje komunikaci pouze určitými protokoly. Pro poštu používáme profesionální MTA (poštovní software) – nejčastěji Postfix, který přesměrovává poštu na lokální SMTP aplikačního serveru TimeMakeru.

Softwarová ochrana aplikačního serveru

Administrační přístupová práva a heslo k serveru mají pouze 2 osoby. Žádná jiná osoba nemá jakékoli oprávnění pro přihlášení k aplikačnímu serveru.

Přihlášení k serveru je možné pouze lokálním přístupem. Vzdálený přístup je umožněn pouze ze dvou přesně definovaných strojů pomocí SSH (šifrovaný přístup), které samy o sobě podléhají dalšímu zabezpečení.

Softwarová ochrana databáze

Databázový server je vetšinou instalován na stejném stroji jako aplikační server. K databázi je umožněn přístup pouze z aplikačního serveru a ze zálohovacího systému. To znamená, že k datům je možný přístup pouze přes systém TM nebo přímo z lokální konzole aplikačního serveru.

DB server obsahuje pouze účet administrátora a účet s minimálními oprávněními nutnými pro běh aplikačního serveru. Administrátorská práva a heslo mají pouze dvě osoby.

Zabezpečený přístup do systému

Přístup do systému je umožněn přes port 443 se stejným počátečním protokolem jako HTTPS, který se po identifikaci příslušného privátního protokolu přepne do interního módu. Komunikace mezi aplikačním serverem a klientem probíhá VŽDY přes SSL vrstvu.

Softwarová ochrana HTTPS serveru

Alternativně mohou běžet na serveru další aplikace, přes HTTP nebo HTTPS server. Protože HTTPS port je již používán pro TM, beží webový server Apache na alternativním portu 444, nebo v případě, že server má více přiřazených IP adres (typické pro hosting), běží každý server na jiné IP.

HTTPS server je spuštěn s přísným bezpečnostním oprávněním.

Vnitřní ochrana systému

Systém přístupových práv

Ke každé akci v systému je definováno přístupové oprávnění. Množství oprávnění není limitováno. Oprávnění lze hierarchicky přiřazovat jednotlivým pracovním pozicím v rámci firmy nebo jednotlivým uživatelským skupinám.

Přístup k přiřazení oprávnění jednotlivým uživatelům mají pouze oprávněné osoby – administrátoři systému.

Omezení přístupu k datům

V systému jsou zahrnuta pravidla, která umožňují definovat rozsah dat, ke kterým daný uživatel může přistupovat (např. podle příslušnosti do organizační struktury firmy).

Offline mode

TimeMaker se synchronizuje s aplikačním serverem a drží si lokálně na počítači kopii té části dat ze serveru, která je pro něj relevantní (má na ni práva a není stará). To umožňuje:

1) Plnohodnotnou práci offline,
2) Oprace se provádějí okamžitě, bez závislosti na rychlosti připojení, synchronizace se provádí na pozadí.

Změny na serveru jsou oznamovány připojeným uživatelům, takže ti je vidí okamžitě (například pokud někdo pošle úkol, vloží pouze záznam do databáze a server tuto změnu rozešle uživatelům, kterých se úkol týká; těm se pak úkol zobrazí v Inboxu nebo na TM Matrixu).
Synchronizace probíhá inkrementálně – přenášejí se pouze rozdíly mezi verzí dat na serveru a lokální kopií.

Zálohování

Záloha probíhá každých 10 minut použitím zálohy aplikačního change logu databáze a nových souborů. Tím je zajištěna kontinuita dat. Jednou týdně se dělá kompletní backup databáze.

Technické výhody systému TimeMaker

snadná a rychlá implementace
automatické aktualizace software
úplný offline režim klientů
jednoduchá administrace systému
šifrovaná komunikace a systém oprávnění