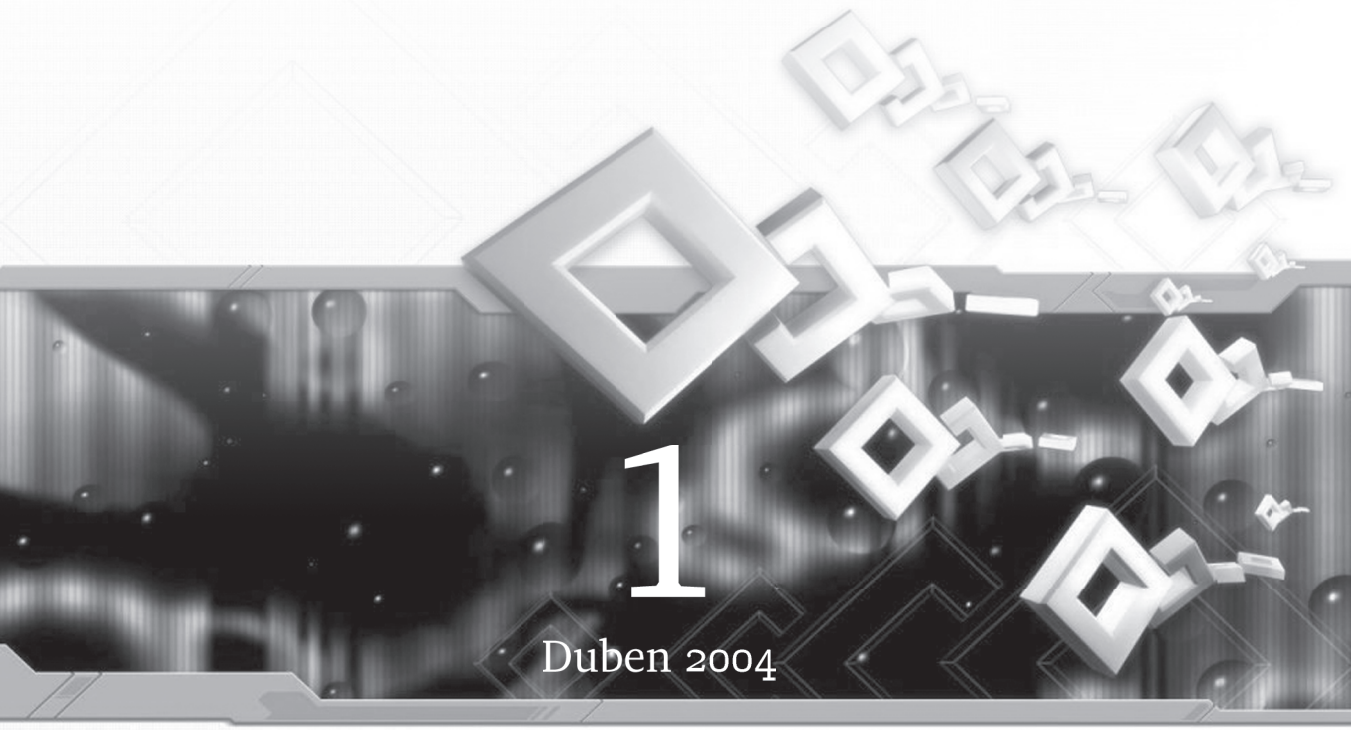
Západočeská univerzita v Plzni
Centrum informatizace a výpočetní techniky

Informační Bulletin
CIV

Rukověť správce
pracovní stanice



1

Duben 2004

Západočeská univerzita v Plzni
Centrum informatizace a výpočetní techniky

Informační Bulletin

1

Duben 2004

Příspěvky uvedené v bulletinu jsou dílem kolektivu autorů CIV.
Publikace neprošla jazykovou ani grafickou úpravou.

Redakční rada: J. Sitera, J. Valdman a L. Kejzlar.

Sazba písmy Bitstream Charter a Concrete v systému LaTeX 2_ε.
Vytiskl TYPOS — Digital Print s.r.o., závod Plzeň.

Vydání první, náklad 350 výtisků.
Vydala Západočeská univerzita v Plzni.

ISBN 80-7043-286-1

Obsah

Kapitola 1

Rukověť správce pracovní stanice

Svět počítačové techniky se stává stále výkonnější, dostupnější a bezohledně pronikající do všech oborů. Ať chceme nebo ne, výpočetní technika nás stále více obklopuje, dovoluje nám výzkum v nových směrech a zaměřeních, dokonalejší organizaci práce, dříve nepředstavitelné možnosti komunikace a agresivně proniká i do soukromého života (mobilní telefon je také malý počítač). Ohromné množství informací, které nabízí Internet, je šancí (ale může být i pohromou) pro každého. Využívat výpočetní techniku není však zadarmo. Tím nejsou myšleny pouze finanční náklady, ale hlavně čas každého z nás, který věnujeme tomu, aby naše „písíčko“, digitální organizátor nebo i již zmíněný mobil pracovaly podle našich představ, zkrátka byly správně nakonfigurovány.

To většinou vyžaduje určitý stupeň znalostí, které není možné žádat po každém. Na každé fakultě, katedře existuje člověk (nebo by měl existovat) v hantýrce často nazývaný „guru“, který má na starosti výpočetní techniku a který správné konfigurace a nastavení udržuje. Právě takovým lidem je určen tento sborník CIV, aby poskytl potřebné informace o možnostech služeb poskytovaných v univerzitní síti, o správné konfiguraci koncových stanic a o strategii a doporučeních CIV. Sborník je ale určen i všem pokročilým uživatelům, kteří se starají o svoji stanici sami.

Sborník tedy není primárně určen běžným uživatelům, neobsahuje ani informace týkající se uživatelské konfigurace jednotlivých služeb, ale je zaměřen na konfigurace a úkony, které se vztahují k pracovní stanici či programovému vybavení (a obvykle je k jejich provedení i třeba mít příslušná administrátorská oprávnění). Sborník se také nezabývá službami pro pracoviště informačního systému ZČU sdružené v distribuci ORIONT–IS.

Hledáte-li informace týkající se uživatelského pohledu na nabízené služby, potom obraťte svoji pozornost na sborník CIV číslo 3/2003. Hledáte-li základní informace o tom, které služby vám CIV poskytuje a jak získat konto pro jejich využívání, doporučujeme vám začít sborníkem „První krůčky“ (2/2003), který je na tuto problematiku specializován.

Řada informací obsažených v tomto sborníku je technického rázu. Může však sloužit také jako základní informace o možnostech využití služeb CIV při plánování technického zabezpečení katedrálních či fakultních pracovišť. Zde je zásadní projekt OPEN ORION, který si klade za cíl poskytnout „instantního“ klienta pro služby ORIONu v konkrétních koncových operačních systémech (kap. 4 a 5), a nabídka služby napojení Windows domény na centrální autentizační službu a bázi uživatelských kont (kap. 3.6).

Kapitola 2 sdružuje informace, které by si měl přečíst každý, kdo se stará o pracovní stanici připojenou do univerzitní sítě. Jsou zde popsány základní služby ORIONu nezbytné pro správné fungování stanice i povinnosti a doporučení, kterými se bude řídit každý zodpovědný správce stanice. Kapitola 3 se zabývá popisem hlavních služeb výpočetního prostředí ORION, které může stanice využívat. Jejich zpřístupnění je možné jak formou klienta OPEN ORIONu popsaného v kapitolách 4 a 5, tak ručně na základě uvedených a odkazovaných informací.

KAPITOLA 2

STANICE VE WEBNETU

Tato kapitola obsahuje informace, které by si měl přečíst každý, kdo se stará o pracovní stanici připojenou do univerzitní sítě. Jsou zde popsány základní služby, které každá stanice potřebuje, ale hlavně úkony, které jsou v síti WEBnet považovány (ať už formálně či neformálně) za povinné a doporučení, kterými se musí řídit každý zodpovědný správce stanice.

2.1 PŘIPOJOVÁNÍ STANIC DO WEBNETU

Univerzitní síť WEBnet je tady proto, aby umožnila kvalitní a rychlé připojení pracovních stanic zaměstnanců, katedrálních a fakultních serverů a v omezeném rozsahu i stanic studentů (viz dále) do Internetu. Je však potřeba dodržet několik základních pravidel a podmínek. Připojovaná stanice musí splňovat nejen technické podmínky připojení, ale i její používání po celou dobu připojení musí být v souladu s pravidly pro používání sítě WEBnet. Zde jsou zásadní dvě věci – platné podmínky pro připojení do akademické sítě CESNET (velmi zjednodušeně řečeno „akademičnost“ činnosti připojené stanice či serveru) a zodpovědnost za „chování“ stanice jako celku vzhledem k ostatním (zejména úmyslné či neúmyslné škození ostatním).

2.1.1 ZÁKLADNÍ POSKYTOVANÉ SLUŽBY

Kromě vlastního připojení do sítě WEBnet (a tím i vysokorychlostního připojení do celého Internetu prostřednictvím národní sítě pro vědu a výzkum CESNET2, `http://www.cesnet.cz`) dostane každá připojená stanice svoji pevnou IP adresu a DNS jméno. K převodu symbolických jmen na IP adresy a obráceně slouží služba DNS zajišťovaná ve WEBnetu několika jmenými servery. Dále je zde služba DHCP pro automatickou konfiguraci stanice[1] po startu používaná zejména notebooky – viz dále.

Doporučená konfigurace DNS pro doménu `zcu.cz` na stanici je shrnuta v následující tabulce – pozor, na pořadí serverů záleží.

Lokalita	**Doporučené jmenné servery**
Bory	147.228.52.17, 147.228.52.11, 147.228.14.10
Centrum města	147.228.14.10, 147.228.221.12, 147.228.52.17
FPE Klatovská	147.228.150.10, 147.228.150.12, 147.228.52.17

[1] samozřejmě jen řádně zaregistrované

2.1.2 ZVLÁŠTNÍ PŘÍPADY

Obecně vzato popisuje obsah této kapitoly připojování katedrálních a fakultních stanic a serverů (pracovní stanice, učebny, servery), přičemž připojování vlastních zařízení studentů je obecně zakázáno. Výjimky existují:

- Studentské koleje – zde je připojování stanic studentů obecně povoleno, technická a organizační stránka podléhá studentské samosprávě. Připojení kolejí je však omezeno jako celek (na rozdíl od jiných částí WEBnetu nejsou stanice studentů z Internetu viditelné apod.). Více viz `http://support.zcu.cz/webnet/koleje.html`
- Služba připojení studentských notebooků – připojování studentských notebooků ve speciálním režimu na vyhrazených místech (mohou být zřízena i na katedrách). Zde je dovoleno plné dočasné připojení do internetu, ovšem až po absolvování dvoufaktorové autentizace (JIS karta, ORION autentizace heslem). Více viz `http://support.zcu.cz/webnet/notebooky.html`

Ve všech ostatních případech nese plnou odpovědnost za chování všech počítačů a zařízení připojených k WEBnetu katedra (nebo jiný útvar), ve které byla „dočasná“ (zejména studentská) zařízení připojena.

2.2 POVINNOSTI SPRÁVCE STANICE

Při připojování stanice k WEBnetu má její správce následující povinnosti:

- *Vlastní fyzické připojení* realizované odpovídající technologií a způsobem. Jiné připojení než do existující oživené sítové zásuvky (např. pomocí vlastního rozbočovače či přepínače) doporučujeme provádět výhradně po konzultaci s pracovníky CIV.
- *Registrace stanice* – každé zařízení připojené do sítě musí být registrováno. Během registrace dostane přidělenu IP adresu (jedinou,kterou smí používat) a DNS jméno. Registrací také informujete CIV kdo je za danou stanici resp. server zodpovědný a kde se nachází. Více viz kap. 2.3.
- *Řádná konfigurace stanice a zabezpečení proti napadení* – správce stanice je povinen zajistit, aby stanice nebyla zneužita pro napadání jiných stanic či šíření problémů. Proto je v jeho zájmu aplikovat základní doporučená opatření. Jedná se zejména o nasazení rezidentního antivirového štítu (kap. 2.4.2), správnou konfiguraci OS (kap. 2.4.1) a poskytobaných služeb (kap. 2.4.5), opatření k zajištění pravidelné (bezpečnostní) aktualizace OS (kap. 2.4.3) a personální firewall (kap. 2.4.4).

2.3 REGISTRACE STANIC

Registrace osobních počítačů je triviální záležitost, kterou většina správců již zná. Žádost o registraci lze podat prostřednictvím formuláře `http://support.zcu.cz/dns` nebo zaslat el. poštou na adresu `hostmaster@service.zcu.cz` například ve tvaru:

```
KATEDRA: KKS
FAKULTA: FST
MISTNOST: UK118
SEGMENT: 41
HW_ADDRESS: 00106a64daed
OPERACNI_SYSTEM: Win2k
MACHINE_TYPE: PC
```

Toto je *doporučený* způsob registrace počítačů, tj. obsahuje informace o *místnosti*, *segmentu*, *katedře*, *fakultě* a *HW adrese*.

Notebooky jsou speciálním případem – s notebookem obvykle uživatelé cestují a někteří jej chtějí provozovat na více místech sítě WEBnet (typicky na katedře, v posluchárnách, na rektorátu apod.) V tomto případě jen připojte řádky:

```
NOTEBOOK_DHCP: ANO
SEGMENTY: 63, 3, 71 a ještě přednáškové místnosti
```

Notebook bude zaregistrován pro použití na uvedených segmentech.

2.3.1 ZJIŠTĚNÍ POTŘEBNÝCH INFORMACÍ

V případě, že neznáte segment, na kterém budete počítač provozovat, zeptejte se lokálního správce IT. Může se stát, že ani on nebude o segmentu vědět (to by však nemělo nastat!) a tak do žádosti napište, že segment vám není znám. My se pokusíme segment dohledat sami.

HW adresu (MAC adresu) lze zjistit pomocí volání `ifconfig` (prostředí UNIX) nebo `ipconfig /all` (prostředí Windows). Následuje vysvětlení některých pojmů:

IP adresa je 32bitové číslo udávané po bajtech v dekadickém tvaru, například 123.213.231.222. Každý počítač v Internetu má IP adresu. Představte si IP adresu jako telefonní číslo. Na ZČU mají všechny počítače adresu začínající na **147.228**.

DNS jméno je symbolické jméno ve tvaru jmeno.firma.cz (v případě ČR). DNS jméno je obvykle svázáno s IP adresou. Představte si DNS jméno jako položku jména v telefonním seznamu vašeho telefonu – nepamatujete si přeci všechna čísla, na rozdíl od jmen? Na ZČU končí DNS jméno řetězcem **zcu.cz**

HW adresa, MAC adresa je adresa síťové karty. Obvykle se zapisuje ve tvaru šesti hexadecimálních čísel, například `00:12:23:DE:AD:F0`. Proč registrovat HW adresu? Protože klientské stanice si nemusejí konfigurovat IP ručně, stačí použít bootp nebo DHCP klienta – což je ve většině operačních systémů proces zcela automatický.

segment, segment sítě laicky řečeno a jen z pohledu sítě WEBnet je to *třetí* číslo IP adresy. Takže stroj `147.228.63.31` je na segmentu *63*.

DNS alias umožňuje dát více jmen jedné IP adrese jako tzv. alias. Například stroj titan.zcu.cz má další jména www.zcu.cz a ftp.zcu.cz.

2.3.2 PROČ JE REGISTRACE POVINNÁ?

I dostáváme se k tomu, *proč* potřebujeme vědět tyto informace – proč prostě nenecháme možnost připojit každému počítač do sítě?

Začneme trochu zeširoka. CIV zodpovídá za adresní prostor univerzity, za IP adresy v rozsahu 147.228.0.0 až 147.228.255.255. To znamená, že problémy z naší sítě směrem *ven* z univerzity padají na hlavu CIVu.

Když se stane nějaký problém (šíření virů, spamů, pokusů o napadení atd.), musí CIV *urychleně* jednat: lokalizovat počítač, zjistit komu patří a zkontrolovat, zda neobsahuje viry nebo jestli není napaden. Zjistíme-li, že stroj *je* napaden, pak je třeba počítač *vyčistit*, tj. odvirovat nebo odstranit problematický software. Nezřídka je jedinou možností kompletní reinstalace stanice.

Kdyby stanice v síti WEBnet nebyly registrované, tj. neměly by záznam, ze kterého je patrno, kde se *fyzicky* nacházejí, byl by velký problém stanici dohledat. Na příkladu (viz výše) stanice s HW adresou `00106a64daed` je na pohled zřejmé, kde se nachází, které katedře patří, a obvykle stačí jeden telefonát, abychom celou záležitost vyřešili.

Existují výjimky z tohoto pravidla. Jsou jím obvykle servery, které nemají ve jméně uvedenou místnost (jak chcete zjistit, kde se nachází stroj `jumbo.fav.zcu.cz` podle jména?). Za takové servery jsou

obvykle zodpovědné osoby na katedře/fakultě, jejichž jméno nebo kontakt je CIVu znám a/nebo mají DNS alias ve stejné formě, jako osobní stanice uživatelů.

Další výjimkou, kterou ovšem neradi vidíme, je chvilkové přidělení nějaké volné neregistrované IP adresy stroji, který bude připojen do sítě WEBnet na krátkou dobu. Je zřejmé, že není třeba registrovat HW adresu stroje, který bude připojen k síti jen pár hodin. Ale prosím pozor! Někdy – až nešťastně často – se stává, že takto *dočasně* připojený stroj je v provozu déle než pár dnů s neregistrovanou IP adresou. Když nastane problém s takovým strojem, *velmi* těžko se dohledává.

? Co CIV dělá v případě, že nemůže dohledat osobu zodpovědnou za stanici?
Nelze-li v rozumném čase dohledat zodpovědného správce nebo uživatele napadeného počítače nebo nastane-li problém u neregistrované IP adresy, nezbývá CIVu nic jiného než:

- zablokovat IP adresu na páteřním směrovači. Toto řešení je nedostačující, protože stroj může dál napadat ostatní stroje univerzity
- zablokovat port na posledním aktivním prvku směrem k napadenému počítači. Počítač pak nemůže napadat zbytek univerzity. Někdy se však stane, že do portu na posledním aktivním prvku je připojeno více strojů – například rozbočovač nebo katedrální přepínač, přes který je napadený počítač připojen. Tímto řešením odpojíme více strojů, ale zbytek univerzity bude ochráněn.

V případě problému na CIV padne těžká volba: buď složitě blokovat IP adresu útočníka nebo zablokovat port na našich aktivních prvcích. Obvykle přistupujeme ke druhému způsobu a blokujeme port nehledě na případné problémy s ostatními počítači, a tím chráníme zbytek univerzity.

! Důležitou změnou, kterou CIV plánuje, je důslednější kontrola neregistrovaných IP a HW adres. V případě nalezení neregistrovaných strojů bude CIV postupovat razantněji a hrozí odpojování takových strojů *předtím*, než způsobí nějaké problémy.

Více informací o DNS, BOOTP, DHCP naleznete na URL: `http://support.zcu.cz`, kde se také nachází seznam aktuálně zablokovaných IP adres a zavirovaných počítačů (tj. potenciálně zablokovaných IP adres :-)

! Všechny počítače ZČU mají být zaregistrovány. Dojde-li ke změnám jako jsou přesuny strojů mezi místnostmi, změna síťové karty (nebo výměna základní desky s on-board síťovou kartou) – měl by uživatel nebo správce tuto změnu nahlásit na standardní adresu. Jestliže tak neučiní, hrozí odpojení počítače od sítě WEBnet.

2.4 OCHRANA STANICE PROTI NAPADENÍ

K zavirovanému nebo hackery napadenému počítači, jehož uživatel nebo správce nám není znám, se chováme jako k počítači, který napadá ostatní infrastrukturu sítě WEBnet a můžeme jej odpojit od sítě. Pokud je správce nebo jiná zodpovědná osoba známa, je vyžadováno okamžité řešení vzniklé situace. Zodpovědnost za takto problematický stroj samozřejmě nese jeho správce či uživatel i v případě, že na problém nebyl pracovníky CIV upozorněn. Nezbývá než přijímat *preventivní* opatření.

Důležitou zásadou je věnovat pozornost všem počítačům ve vaší správě. I nejposlednější počítač v rohu kanceláře, který používáte jednou za měsíc, může být hrozba pro bezpečnost ostatních počítačů (nejen) v síti WEBnet. Stejně tak počítač, který připojujete k síti jen dočasně (notebook), může být velmi dobře napaden.

Filozoficky je akademická sítě ZČU velmi otevřená. To však neznamená jen velkou svobodu užívání sítě, ale i velkou zodpovědnost. Hlavní díl zodpovědnosti připadá na samotné uživatele (protože především jejich chování je navenek vidět), ale velká část je i na správcích stanic. Je totiž nezbytné, aby se správci stanic aktivně podíleli na „čistotě“ univerzitního prostředí kvalitní péčí o bezpečnost svých stanic.

! V případě podezření na napadení svého systému jej nejprve odpojte od počítačové sítě a teprve potom se zabývejte identifikací problému nebo hledáním pomoci.

! V případě zjištění nevhodnémho chování uživatelů (WEBnetu i jiných sítí) se obraťte na CIV (prostřednictvím `operator@service.zcu.cz` nebo `abuse@zcu.cz`).

Stejně jako řešíme stížnosti na chování našich uživatelů, jsme zde i od toho, abychom informovali správce jiných sítí o problémech u nich a žádali nápravu.

2.4.1 ODPOVÍDAJÍCÍ KONFIGURACE OS

Prvním důležitým doporučením je omezení anonymního přístupu na stanici a vymazání standardních uživatelů jako je `guest`. Důležitá je okamžitá změna administrátorského hesla na nové, netriviální heslo podle známých doporučení (viz např. sborník CIV 3/2003). V moderních operačních systémech je již situace po instalaci zpravidla výrazně blíže těmto doporučením, než tomu bylo dříve. Proto doporučujeme nepoužívat starší OS (zejména Windows 9x).

Další v řadě bezpečnostních doporučení je provozování jen takových služeb, které jsou bezpodmínečně nutné k provozu počítače. Je jasné, že provozování www a ftp serveru na stanici sekretářky je zcela zbytečné a potenciálně nebezpečné. Z hlediska běžné stanice uživatele není důvod, aby na OS běžela nějaká služba a prakticky všechny služby můžeme zastavit. V prostředí Microsoft Windows jsou to převážně služby pro sdílení disků a tiskáren. Rozhodnete-li se přesto provozovat sdílení disků, je velmi vhodné omezit jej personálním firewallem (kap. 2.4.4). V unixových OS jsou to převážně služby spouštěné pomocí `inetd` jako například telnet, rsh, neanonymní ftp. Dále pak jsou to služby `portmapper` a NFS tam, kde to není potřeba. Standardní OS typu UNIX se dodávají i s DNS serverem `bind`, který také není potřeba na stanici provozovat.

Sdílení počítačových prostředků (zejména disků a tiskáren) je obecně povoleno, doporučujeme si však řádně promyslet řízení přístupu k těmto prostředkům. Obvykle tím rozumíme zpřístupnění disků a tiskáren jen v rámci jedné katedry (což je ideální aplikace pro personální firewall).

Správci lokálních sítí by měli klást důraz na používaní bezpečných verzí programů a protokolů jako jsou ssh verze 2 (namísto protokolů telnet a ssh verze 1) pro terminálový přístup nebo Secure POP a Secure IMAP, namísto protokolů POP a IMAP (což ve stávajících programech pro čtení pošty znamená jen triviální změnu konfigurace).

Tam, kde je nutné používat nezabezpečené protokoly, je vhodné omezit nebo řídit přístup pomocí osobního firewallu nebo uvažovat o zřízení virtuálních privátních sítí. Pro správný chod univerzitní sítě WEBnet je důležité, aby se uživatelé chovali v rámci pravidel této sítě. V případě, že budou používat nestandardní programy, speciální aplikace nebo provozovat internetovské servery, je vhodné se o tom nejprve poradit s lokálním správcem sítě nebo kontaktovat přímo CIV prostřednictvím operátorské služby `operator@service.zcu.cz`.

2.4.2 ANTIVIROVÝ ŠTÍT

ZČU má zakoupenou celouniverzitní licenci k antivirovému software AVAST32. Tento software může použít *každý* zaměstnanec ZČU *bez* toho, aby musel za licenci platit. Z pohledu CIVu proto není zcela pochopitelné, že se na síti WEBnet vyskytují stroje, které antivirový program *nemají* nainstalován.

Aby antivirový program fungoval správně, musí být *pravidelně* aktualizován. Správná konfigurace tedy obsahuje nastavení pro automatickou aktualizaci „virové databáze“ každý den. Alternativou je navyknout uživatele, že aktualizace antivirového programu patří k ranním rituálům jako je ranní káva nebo čtení elektronické korespondence. I sebelepší antivirový program potřebuje aktuální informace o nových virech a hrozbách, bez nichž je velmi málo účinný.

Stejně tak platí, že aby byl účinný, musí antivirový program běžet v rezidentním režimu tj. stále na pozadí (rezidentní štít, který kontroluje činnost celého systému). Ostatní režimy antivirového programu jsou pro dnešní agresivní prostředí Internetu použitelné obvykle pro analýzu post-mortem, neboli až poté, co byl počítač napaden.

Více informací naleznete na URL: `http://support.zcu.cz/av`

! Všechny počítače s OS Windows musí mít nainstalován antivirový program, který běží v rezidentním režimu a má řádně aktualizovanou virovou databázi.

2.4.3 AKTUALIZACE OS

Velmi důležitý úkol správce stanice či jejího uživatele je pravidelná aktualizace OS. Většina dnešních OS již zahrnuje prostředky pro jednoduchou aktualizaci jako jsou například služba Microsoft Update nebo v prostředí OS Debian Linux příkaz `apt-get update, apt-get upgrade`. Uživatelé by měli být seznámeni s touto službou a měli by jí pravidelně používat.

! Neaktualizovaný OS je potenciálně stejně nebezpečný jako zavirovaný počítač!

Použití personálního firewallu výrazně snižuje riziko napadení stanice s neaktualizovaným OS, nicméně naše doporučení zní: používejte obojí. Jen tak lze využít potenciál těchto opatření naplno, neboť vznikne dvouúrovňová ochrana. Spoléhání se pouze na personální firewall může mít svá úskalí.

2.4.4 PERSONÁLNÍ FIREWALL

Doporučená konfigurace personálního firewallu pro prostředí ZČU je taková, která omezí přístup na váš počítač a minimálně omezí přístup aplikací z vašeho počítače kamkoli do světa. Například typická konfigurace pracovní stanice může vypadat takto:

- povolit veškerou komunikaci z adresy 127.0.0.1 (loopback, neboli počítač se může spojit sám se sebou)
- povolit veškerou odchozí komunikaci
- povolit komunikaci, která je navázaná směrem ze stanice nebo je tzv. příbuzná (protože UDP je bezstavový protokol, nelze jednoduše navázat *spojení* – proto *příbuzné spojení*)
- zakázat veškeré spojení na pracovní stanici z Internetu

V zápisu paketového filtru `iptables`, používaném v Linuxu je tento zápis:

```
iptables -A INPUT -i lo -s 127.0.0.1 -j ACCEPT
iptables -P OUTPUT  ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -P INPUT DROP
```

Druhé pravidlo není potřeba – je takto nastaveno standardně a uvádíme ho jen z pedagogických důvodů. V případě, že chcete, aby stanice byla "vidět", tj. aby odpovídala na ICMP zprávy, pak přidejte pravidlo:

```
iptables -A INPUT -p icmp -j ACCEPT
```

Máte-li problémy se službou FTP (přihlášení k FTP serveru trvá dlouhou dobu), pak přidejte ještě pravidlo:

```
iptables -A INPUT -p tcp --dport 113 -j REJECT
```

2.4.5 ZABEZPEČENÍ KATEDRÁLNÍCH A FAKULTNÍCH SLUŽEB (SERVERŮ)

Servery poskytující služby vyžadují poněkud jiný přístup než koncové stanice, základní pravidla zde však platí stejná. Zejména je žádoucí řádná registrace včetně odpovídajícího technického kontaktu (abychom věděli co dělat v případě problémů) a odpovídající zabezpečení proti napadení (aby problémy nenastaly). Ochrana personálním firewallem je účinná pouze omezeně (nemůže chránit poskytované služby), proto je zásadní zejména včasná aktualizace SW.

Předtím, než se rozhodnete na katedře/fakultě provozovat nějakou službu vlastními prostředky, je rozumné se seznámit se službami, které poskytuje CIV: například certifikační autorita (kap. 2.5.1), virtuální weby (kap. 3.7.2) a další. Ve většině případů vás využívání služeb CIV nic navíc nestojí, nijak významně vás neomezuje a navíc vám odpadne starost s konfigurací, zabezpečením a aktualizací SW. Detailní přehled služeb CIV naleznete na `http://sluzby.civ.zcu.cz`

2.5 SLUŽBY SOUVISEJÍCÍ S PŘIPOJENÍM A ZABEZPEČENÍM STANIC

2.5.1 CERTIFIKAČNÍ AUTORITA ZČU

CIV poskytuje služby certifikační[2] autority pro uživatele, stanice a servery sítě WEBnet. V případě, že uživatelé používají e-mailové služby, pak se již s certifikační autoritou setkali v případě certifikátu poštovního serveru (viz `http://mail.zcu.cz/dokumentace/certifikaty.html`). Pro hladký běh aplikací, které používají certifikáty vydané naší autoritou, je vhodné nainstalovat (podle výše uvedeného návodu) certifikát naší certifikační autority na všechny počítače, které tyto aplikace používají.

Jestliže správci sítě potřebují ke běhu svých služeb (HTTPS server, Secure POP, IMAP, zabezpečení jiných služeb pomocí SSL) certifikát, vydaný certifikační autoritou ZČU, pak mohou kontaktovat správce certifikační autority na adrese `aaa-req@service.zcu.cz` a ten jim certifikát vystaví nebo podepíše.

2.5.2 PŘIPOJOVÁNÍ WIFI ZAŘÍZENÍ

Vizí CIV je chápat bezdrátové sítě jako další, poněkud specifický, prostředek k připojení koncových zařízení do sítě WEBnet. Technologická specifika tohoto způsobu připojování vedou ještě více k potřebě centrální koordinace, než tomu je u klasické kabeláže. CIV pracuje na několika projektech, na jejichž konci je realizace této vize. Zatím však bezdrátové připojení do WEBnetu s dostatečnou dostupností není k dispozici[3].

Současný stav je takový, že připojování WiFi zařízení (zařízení poskytujících WiFi konektivitu jiným zařízením) do sítě je dovoleno pouze se souhlasem CIV, přičemž se vydává jen časově omezený souhlas. Pracujeme na komplexním řešení, které nabídne vlastnosti přijatelné pro uvedení bezdrátových sítí do běžného života univerzity, ale ani pak nebude možno provozovat v areálu ZČU WiFi přípojné body bez jejich začlenění do centrální infrastruktury. V případě, že katedra nutně potřebuje ke své práci WiFi (i za těchto podmínek), je nezbytné kontaktovat CIV a domluvit se alespoň na základním zabezpečení WiFi sítě (provozovat nezabezpečenou WiFi síť je velmi hloupý nápad).

2.6 ZDROJE INFORMACÍ PRO SPRÁVCE STANICE

2.6.1 SUPPORT.ZCU.CZ

Hlavním zdrojem informací poskytovaných CIV pro správce stanic je server `http://support.zcu.cz`. Jsou zde koncepční dokumenty, návody na instalaci, odkazy na další zdroje informací a mnohé další.

[2] ve zkušebním provozu

[3] Pilotní projekt WiFi připojení je určen pouze studentům a zatím pokrývá jen malou část areálu na Borech. Víte-li o tom, že by se vaše katedra chtěla v průběhu roku 2004 podílet na nasazování WiFi technologií, kontaktujte CIV. Součástí projektu FRVŠ (bude-li přijat) bude i pilotní nasazení pro vybrané části katedrálních prostor.

2.6.2 SYSTÉM RT

Pro řešení problémů a požadavků je jednotným vstupním bodem adresa `operator@service.zcu.cz`. Při vznášení dotazů se prosím snažte co nejpreciznějí popsat svůj problém. Šetříte tím i svůj čas. Pokud jako správce nebo kontaktní osoba řešíte problémy často, věnujte prosím pozornost seznámení se s aplikací *RT systém* (`http://rt.zcu.cz`), která se stará o údržbu informací o jednotlivých dotazech/problémech a umožňuje sledovat stav jejich řešení.

2.6.3 ELEKTRONICKÉ KONFERENCE KONTAKT A WEBNET

Každému správci stanice (i uživatelům) doporučujeme zapsat se do konference `webnet@list.zcu.cz`. Z této konference budete dostávat upozornění na důležité události v „životě“ sítě WEBnet. Návod na přihlášení do konference najdete na `http://mail.zcu.cz/dokumentace/konference.html`. Pokud vám nevyhovuje forma elektronické konference (dostáváte e-maily s informacemi), doporučujeme alespoň pravidelně sledovat sekci novinky na webu `http://support.zcu.cz`.

! Konference `kontakt@list.zcu.cz` je určena kontaktním pracovníkům kateder v oblasti IT. Všechny útvary, katedry a fakulty by zde měly mít svého zástupce.

Zasílané informace mají podobný charakter jako v případě konference WEBNET, konference je však uzavřená a její členství se určuje na základě nominování zástupce katedry (prostřednictvím aplikace telefonní seznam).

2.6.4 KATALOG SLUŽEB CIV

Všechny služby, které CIV poskytuje uživatelům, jsou popsané a informace o nich jsou dostupné na adrese `http://sluzby.civ.zcu.cz`. Pro přístup k těmto informacím je nezbytné přihlášení ORION jménem a heslem. Věnujte pozornost i zde uvedeným informacím o statutu služby (zkušební provoz, normální provoz, útlum služby).

KAPITOLA 3

SLUŽBY VÝPOČETNÍHO PROSTŘEDÍ ZČU

Následující dvě kapitoly (4, 5) popisují programové balíky realizující klientskou instalaci hlavních služeb prostředí ORION v „instantním“ provedení, tj. převážně zcela automatizovanou. Tyto balíky CIV připravil pro zjednodušení vaší práce, udržuje je však pouze pro některé operační systémy na vaší stanici.

Základní obecný popis poskytovaných služeb včetně konkrétních údajů (vztahujících se ke službě, nikoli k nastavení jednotlivých klientských OS) je obsažen v této kapitole. Tento popis slouží pro vaši informaci v případě řešení problémů či pokud se rozhodnete o konfiguraci klientského prostředí bez použití instalačních balíků.

Všechny níže uvedené služby poskytuje CIV potenciálně každému zaměstnanci a studentovi ZČU. Způsob a podmínky získání uživatelského konta a podpora poskytovaná koncovému uživateli, to jsou vše věci přesahující rámec tohoto sborníku a lze je nalézt v jiných publikacích, které CIV vydává. Níže uvedené informace u jednotlivých služeb jsou vybrány s ohledem na zájem správce klientského systémového a aplikačního programového vybavení.

3.1 ÚVOD – INFORMACE O PROJEKTU OPEN ORION

Projekt OPEN ORION je vyjádřením jedné ze snah o rozvoj výpočetního prostředí ZČU (projekt ORION) s ohledem na současnou situaci a potřeby. Jeho hlavní myšlenkou je využití vývoje v okolním světě, kde dochází k stále silnější akceptaci technologií, jež jsou klíčovými stavebními kameny projektu ORION, pro výrazné vylepšení podpory uživatelů s vlastní stanicí (pod vlastní správou) snadno aplikovatelnou formou (zjednodušeně řečeno ORION klientem pro jejich OS).

3.1.1 STRUKTUROVANÉ NASAZENÍ PROJEKTU ORION

Projekt ORION je postaven tak, aby umožňoval několik variant nasazení své funkcionality na systémech jednotlivých uživatelů. Pro zjednodušení problematiky stanovme následující základní možnosti/kombinace:

a) Plné nasazení

   Systém využívá veškeré funkcionality projektu ORION. Jeho použití a možnosti zcela určuje koncepce a aktuální stav projektu ORION. Centrálně instalovaný SW, konkrétní fixní distribuce operačního systému, transparentní přístup k datům a jednotnému uživatelskému rozhraní ze všech systémů. Mechanismy údržby systému vhodné především pro veřejné laboratoře a centrální přístupové servery.

b) Systém ve vlastní správě

Lokální systém se samostatnou správou, který umožňuje transparentní přístup k datům výpočetního prostředí. Systémový a aplikační SW je udržován lokálně dle potřeb a možností uživatele, systém využívá centrální autentizační službu a souborový systém.

c) Systém s odpovídajícími přístupovými prostředky

Zcela lokální a nezávislý systém. Část instalovaného SW dovoluje bezpečný a plnohodnotný vzdálený přístup k vybraným službám ORIONu.

3.1.2 CÍLE PROJEKTU OPEN ORION

Cílem projektu OPEN ORION je shromáždit a systematicky udržovat informace potřebné pro nasazení dle varianty b) a c). Jedná se zejména o informace na úrovni konkrétních technických popisů pro jednotlivé operační systémy, které v současnosti dovolují relativně přímočaře dosáhnout požadovaného výsledku bez nutnosti hlubších znalostí a zásahů.

Základní cílovou oblastí projektu OPEN ORION jsou uživatelé výpočetní techniky z řad studentů a zaměstnanců ZČU, kteří chtějí přistupovat k základní funkcionalitě univerzitního výpočetního prostředí ze svých pracovních stanic za výše naznačených podmínek.

! Výše uvedená varianta a) v současné době představuje systémy nasazené na centrálních uživatelských serverech, ve veřejných učebnách CIV (ORIONT, ORION LINUX a na pracovištích IS používajících ORIONT–IS).

3.1.3 VARIABILITA NASAZENÍ PROJEKTU OPEN ORION

I v rámci projektu OPEN ORION je možná variabilita v míře použití jednotlivých služeb. Kromě členění naznačeného výše variantami b) a c) existuje ještě podrobnější možnost rozhodnutí správce stanice ve variantě b). Lze například udržovat lokálně uživatelská konta a využívat pouze centrální autentizační služby (není třeba udržovat lokálně hesla), nebo se lze rozhodnout i pro použití centrální služby distribuce uživatelských účtů. V obou případech je možné jak využití lokálního diskového prostoru, tak diskového prostoru služby distribuovaného diskového systému.

3.1.4 OPEN ORION – POHLED UŽIVATELE

Uživatelem výsledků projektu OPEN ORION je každý, kdo je schopen a ochoten základní systémové správy nějakého (podporovaného) operačního systému (platformy). Vize projektu OPEN ORION je taková, že každý takový člověk musí dostat k dispozici z jeho pohledu jednoduchý a srozumitelný mechanismus pro provedení kroků, jež z jeho OS zpřístupní základní služby poskytované v rámci výpočetního prostředí ZČU. V závislosti na technických okolnostech a platformě může nastat jedna z následujících situací:

- Pro zvolený cíl je k dispozici konkrétní návod, popisující konfiguraci zvolené platformy s použitím běžně dostupného systémového a aplikačního SW. Tento SW může být buď udržován přímo v rámci distribuce OS, nebo třetí stranou (např. Open Source projekt). Návod je udržován lokálně dle specifik výpočetního prostředí ZČU (tj. také náležitě průběžně přizpůsobován změnám).
- Kromě návodu je k dispozici také příslušná SW komponenta realizující majoritu lokálních konfiguračních a jiných přizpůsobení. Smyslem této komponenty je zjednodušení (automatizace) konfiguračních kroků. Podle technických možností může jít o samostatný SW balík realizující konfiguraci a náležité „slepení“ standardních SW balíků[1], nebo také o „lokalizované“ SW balíky (standardní balíky s jinými implicitními konfiguracemi, či vhodnými základními doplňky pro bezstarostnou integraci do výpočetního prostředí ZČU).

[1] Viz kapitola 4, kde je využito závislostí balíků v rámci nástroje DPGK distribuce Linuxu Debian k provázání standardních balíků s programovým vybavením s OPEN ORION balíky, které obsahují specifickou konfiguraci pro služby ORIONu.

- V některých případech musí být poskytováno i specifické SW vybavení. Může jít o komponenty, které nejsou dosud pro danou platformu standardně k dispozici, nebo o nestandardní komponenty, specifické pro výpočetní prostředí ZČU. Zde se může situace průběžně měnit dle vývoje s akceptací technologií jednotlivými platformami.

Uživatel (zde systémový správce lokálního OS) je plně zodpovědný za funkčnost systému a všechny jeho komponenty. Je poskytována technická podpora na nejasnosti a chyby v dokumentaci a řešení případných problémů s výše naznačenými SW balíky.

3.2 ELEKTRONICKÁ POŠTA

Služba elektronické pošty může být kompletně používána bez instalace jakéhokoli SW prostřednictvím klienta založeného na WWW prohlížeči (`http://webmail.zcu.cz`)[2]. Pro běžnou práci však doporučujeme instalaci programu pro práci s poštou, přičemž poskytovaná služba je přístupná standardním protokolem IMAP, případně POP3. Nastavení programu pro práci s poštou může zpravidla provádět sám uživatel, je však vhodné, aby mu správce stanice byl schopen poskytnout pomoc.

3.2.1 ZÁKLADNÍ PARAMETRY PŘÍSTUPU K POŠTĚ

Tento odstavec popisuje nastavení uživatelského účtu v programu pro práci s poštou.

K poště lze přistupovat dvěma protokoly, IMAP a POP3. V obou případech je podporována pouze bezpečná varianta protokolu (zabezpečení přes SSL). Základní nastavení serveru pro poštu je v následující tabulce:

Protokol (typ serveru)	**jméno serveru**	**port**
IMAP	imap.zcu.cz	993
POP3	pop.zcu.cz	995

Dalším důležitým parametrem je server pro odchozí poštu. Jeho nastavení v dnešní době, kdy je třeba se chránit proti zneužití poštovních serverů, závisí na způsobu, jakým je uživatel připojen k síti Internet. Pokud jste připojeni přímo do sítě WEBnet, použijte nastavení z následující tabulky. Pokud jste připojeni jinak, musíte zjistit a použít server poskytovatele vašeho připojení (ISP). Server ZČU (`smtp.zcu.cz`) zprávy odesílané z jiné sítě než ZČU příjemcům do jiných sítí než ZČU odmítá.

Server odchozí pošty (SMTP)	smtp.zcu.cz
Použít zabezpečení	ne (port 25)

Další parametry poštovní služby si nastavuje sám uživatel. Jedná se zejména o přesměrování, třídicí pravidla, antivirovou a antispamovou kontrolu došlé pošty (vše se nastavuje na poštovním serveru).

! Připomeňme i zde nutnost zabezpečení pracovní stanice antivirovým rezidentním štítem (zpravidla souvisí zejména s poštou a přílohami poštovních zpráv), což je úkol správce stanice.

3.2.2 PARAMETRY PRO NASTAVENÍ SLUŽBY ADRESÁŘE ZČU

Elektronický adresář ZČU je přístupný přímo z klientů elektronické pošty protokolem LDAP. Jedná se o stejná data, která najdete přes webovou službu: `http://phone.zcu.cz`. Parametry pro nastavení této služby jsou shrnuty v následující tabulce:

LDAP server (hostname)	ldap.zcu.cz
báze dat (base DN)	ponechat prázdné
autentizace	anonymní přístup
verze LDAP protokolu	2 i 3
zabezpečení SSL	ne (port 389)

[2] Nastavení poštovní služby a archivaci pošty standardně uživatel provádí prostřednictvím WWW adresy http://mail.zcu.cz.

Podrobné návody pro nastavení výše uvedených parametrů v podporovaných klientech elektronické pošty najdete ve sborníku CIV 3/2003, kap. 3 a na URL `http://mail.zcu.cz`.

3.3 TISKOVÉ SLUŽBY

CIV nabízí tiskové služby pro studenty, zaměstnance i podporu tisku pro katedry či jiné útvary ZČU. Poskytované služby jsou založeny na laserových tiskárnách HP, z nichž většina je pronajata v rámci programu PrintAdvantage, a jehličkových tiskárnách EPSON. Rozhraním pro uživatele jsou tiskové fronty realizované tiskovými servery (koncový uživatel zpravidla vidí pouze jméno tiskárny, zde myslíme uživatelem služby správce stanice).

Přístup k tiskovým frontám je realizován protokolem LPR, v unixových OS je k dispozici standardně stejnojmenný příkaz. V MS Windows je tento protokol také standardně podporován, konfigurace tiskárny pouze vyžaduje jistou zkušenost (viz dále).

Tiskové služby jsou samozřejmě přístupné ze všech centrálně udržovaných instalací ORIONu (uživatelské servery, učebny CIV, pracoviště IS). Zde je již provedena konfigurace tiskových front a příslušného softwaru. Na jiných pracovištích musí tuto konfiguraci provést správce stanice. Služba není nijak vázána na ostatní služby ORIONu.

3.3.1 ZÁKLADNÍ PRINCIP KONFIGURACE V MS WINDOWS

Standardně OS Windows LPR podporuje, nicméně primárně počítá s použitím MS sdílení tiskáren. Konfigurace je na první pohled poněkud „málo přímočará“. Rámcový postup je:

- Vytvoření tiskárny standardním průvodcem (průvodce přidání tiskárny), vyberte „*tiskárna je místní, připojená k tomuto počítači*“!
- Nutno vytvořit „port“, což je komunikační bod realizující přístup do tiskové fronty (vytvořit nový port, typ *standard TCP/IP port*).
- Nastavení portu podle níže uvedené tabulky.

Název portu	libovolný dle uvážení (pouze název entity „port“)
Název či adresa IP tiskárny	jméno odpovídajícího tiskového serveru
Protokol	LPR
Název fronty	sem skutečně název odpovídající fronty
Povolit počítání bajtů LPR	ano (zaškrtnout)

Je třeba nainstalovat správné ovladače pro konkrétní typy tiskáren, neboť jen tak umožníte uživatelům používat rozšířené funkce (oboustranný tisk, barevný tisk, atd.). Ovladače použitých tiskáren jsou k dispozici ke stažení na WWW straně dokumentace tiskových služeb (`http://support.zcu.cz/tisk/`), spolu s podrobným návodem (krok za krokem) na konfiguraci LPR tiskárny.

3.3.2 ZÁKLADNÍ PRINCIP KONFIGURACE V OS UNIX (LINUX)

Základní konfigurace v OS typu UNIX je velmi jednoduchá. Není třeba používat zvláštní ovladače (alespoň pokud používáme postscriptové tiskárny), stačí správně doplnit odpovídající řádky v konfiguračním souboru `/etc/printcap`. Tyto řádky jsou k dispozici v globálním konfiguračním souboru na AFS (`/zcu/common/etc` nebo vám je automaticky nainstaluje balík *printorion* popsaný v kap. 4.

3.3.3 PARAMETRY VYBRANÝCH TISKOVÝCH SLUŽEB

Veřejně poskytované tiskové služby[3] mají pevně definované rozhraní, ale přesto může docházet k jistým změnám. Následující informace jsou proto pouze orientační a aktuální stav je třeba zjistit v dokumentaci tiskových služeb. Veřejné tiskové služby v současnosti zajišťují:

- HelpDesk CIV – operátorská pracoviště na Borech (UI205a) a v Husově ulici (HJ306).
- Copy Centrum ZČU – areál Bory (UU011), CIV zde poskytuje pouze technickou podporu tiskové služby.

Jména tiskových front, umístění a parametry tiskáren jsou shrnuty v následující tabulce:

Pracoviště	Jméno fronty	Místnost	Barva	A3/A4	Duplex	Tiskový server	Tiskárna
HelpDesk CIV Bory	bory-cb01	UI205	ne	A4	ano	lpd-civ03.zcu.cz	HP4100
HelpDesk CIV Bory	bory-barva01	UI205	ano	A4	ne	lpd-civ03.zcu.cz	HP4600
HelpDesk CIV Bory	bory-dfx0[1,2]	UI205	ne	A4	ne	lpd-civ01.zcu.cz	DFX5000
HelpDesk CIV HJ	husova-cb01	HJ306	ne	A4	ano	lpd-civ03.zcu.cz	HP4100
HelpDesk CIV HJ	husova-dfx01	HJ306	ne	A4	ne	lpd-civ02.zcu.cz	DFX5000
CopyCentrum Bory	copyc-cb01	UU011	ne	A3,A4	ano	lpd-civ03.zcu.cz	HP8150
CopyCentrum Bory	copyc-barva01	UU011	ano	A3,A4	ano	lpd-civ03.zcu.cz	HP5500

! Všechny tiskárny kromě DFX5000 jsou laserové a podporují PostScript. Tiskárna HP8150 v Copy Centru navíc umožňuje sešívání výtisků. Doporučujeme zvážit použití duplexu (oboustranného tisku) k úspoře papíru, místa i peněz.

Tiskové fronty přijímají úlohy 24 hodin denně, tisk ale probíhá pouze během provozní doby příslušných pracovišť. Tisk na jehličkových tiskárnách CIV probíhá automaticky v pořadí tak, jak jsou jednotlivé tiskové úlohy ve frontě, výtisk si stačí jej vyzvednout. Všechny laserové tiskárny mají nastaven režim pozastavení tisku, tj. po odeslání tisku uživatel musí kontaktovat pracovníka HelpDesku (či CopyCentra), požádat o odblokování úlohy a také zaplatit poplatek za tisk dle vytištěných stran. Pracoviště mohou mít definována ještě podrobnější pravidla pro organizaci služby tisku (např. v CopyCentru možnost bezhotovostní platby katedrami), se kterými se uživatel stejně jako s ceníkem tisku seznámí v příslušné dokumentaci. Úkolem správce stanice je pouze umožnit vytvoření a odeslání tiskové úlohy do fronty tiskového serveru. Speciální vlastnosti tisku (oboustranný tisk, barva) jsou zpravidla záležitostí tvorby tiskové úlohy uživatelem, ale pro jejich jednoduché používání je nezbytné nainstalovat správné ovladače tiskáren (týká se MS Windows – viz výše). Ovladače použitých tiskáren jsou k dispozici ke stažení na WWW straně dokumentace tiskových služeb (`http://support.zcu.cz/tisk/`).

3.4 INSTANTNÍ PŘÍSTUP K INFORMAČNÍMU SYSTÉMU (TENKÝ KLIENT)

Jako doplněk k primární službě pro pracoviště informačního systému školy ORIONT–IS poskytuje CIV službu ORIONTS–IS. Rozdíl je zásadní. První služba je distribuce OS založená na Windows a specializované sadě ORION služeb (s ohledem na potřeby IS a zejména nutnost kvalitní podpory). Druhá služba, ORIONTS–IS, je určena pro zpřístupnění základních aplikací IS z libovolné stanice bez velkých nároků na její konfiguraci či software.

Použitá technologie tenkého klienta zpřístupňuje aplikace ze vzdáleného výkonného terminálového serveru (dále jen TS). To znamená, že aplikace neběží na koncové stanici, ale na vzdáleném serveru a na stanici je z TS otevřeno jen okno aplikace (nikoli tedy celá pracovní plocha, tzv. desktop) – stanice se stará pouze o vstup a výstup aplikace. Tyto aplikace tvoří – STAG (studijní agenda), Magion (účetnictví) a Legsys (sbírka zákonů). Zmíněné aplikace jsou přístupné jako tzv. publikované aplikace. Toto řešení

[3] parametry tiskových služeb kateder je třeba zjistit zpravidla u vlastníka tiskáren

umožňuje zpřístupnit nejnovější software i koncovým uživatelům, jejichž stanice pro něj nemají dostatečný výkon, ale zásadní ve službě ORIONTS–IS je fakt, že toto řešení umožňuje zpřístupnit aplikace bez podstatných nároků na SW konfiguraci koncové stanice při garanci funkčnosti aplikací[4].

Z hlediska úrovně uživatelské podpory je třeba říci, že ORIONT–IS je primární služba pro pracoviště kde se požaduje velká spolehlivost. ORIONTS–IS je doplňková služba s nižší úrovní podpory.

Z hlediska správce stanice je třeba pro provoz služby ORIONTS–IS nainstalovat příslušný SW balík (klient terminálových služeb – více viz dále). Vlastní nastavení klienta může provádět sám uživatel.

3.4.1 PODMÍNKY POUŽITÍ SLUŽBY

Službu ORIONTS–IS je třeba aktivovat pro konkrétní stanici a uživatele, přičemž aktivace je zpoplatněna. Jedná se o jednorázový poplatek 5300 Kč (pokud máte nainstalován operační systém Windows 2000, nebo XP – u starších verzí je cena vyšší kvůli licenci TSCAL – tj. 6800 Kč)

O zprovoznění tenkého klienta požádejte HelpDesk CIV (nejlépe prostřednictvím RT, e-mailem na operator@service.zcu.cz, nebo na tel. čísle 37763 8888). Operátoři váš požadavek předají kompetentním osobám a ty vám službu zpřístupní. To probíhá tak, že se zaregistruje vaše IP adresa a povolí uživatelské jméno. Poté dostanete mail, že registrace proběhla a budete v něm rovněž vyzváni ke kontrole funkčnosti (potřebujeme ověřit, že vám služba běží a nevyskytují se problémy).

Před aktivací služby je třeba:

- mít zřízené konto v univerzitním prostředí ORION,
- znát IP adresu stroje na kterém požadujete tenkého klienta (zjistí se zadáním příkazu `ipconfig` (Windows) nebo `ifconfig` (Linux) na příkazové řádce),
- znát informace pro vnitrofakturaci (číslo střediska, zakázky)

3.4.2 TECHNICKÉ INFORMACE PRO POUŽITÍ SLUŽBY

Všechny informace a návody najdete na stránce `http://support.zcu.cz`. V této kapitole jsou pouze pro vaše pohodlí uvedeny základní informace.

INSTALACE ICA KLIENTA

ICA klient existuje pro různé platformy. Na AFS by měly být k dispozici nejnovější verze v adresáři `/afs/zcu.cz/software/services/ica/icaclnt` nicméně klienta je možné stáhnout přímo z webu `http://www.citrix.com`, sekce download. Soubor si uložte na disk a spusťte – nainstaluje se vám ICA klient. Na ploše (pokud jste to nezrušili) vám přibude ikona Citrix Program Neighborhood – místo pro nastavení ICA klienta. (v UNIXu je to "wfcmgr").

NASTAVENÍ ICA KLIENTA

Nejprve otevřete Citrix Program Neighborhood a vyvolejte dialog z menu File → Custom Connection Settings, ve kterém se nastavují globální parametry pro všechna ICA spojení.

- V položce *Network Protocol* nastavte `TCP/IP`.
- *Server Group* ponechte `primary`.
- Do seznamu *Address List* přidejte tlačítkem Add tyto adresy:
  `prometheus.xp.zcu.cz, atlas1.xp.zcu.cz, atlas2.xp.zcu.cz, atlas3.xp.zcu.cz`

[4]Garance funkčnosti v pojetí ORIONT–IS je závislá na konkrétní omezené škále instalovaného SW a nemožnosti zásahů do konfigurace stanice ze strany uživatele.

- V záložce Default Options:
  - Položku *Encryption Level* nastavte na `basic`.
  - *Window Colors* na `256 Colors`.
  - *Window Size* na `800 × 600`.

V unixovém klientu se vše nastavuje z dialogu, který získáme z menu Option → Settings... Položky a hodnoty, které je třeba nastavit v podstatě korespondují s nastavením jako u Windows klienta, které bylo popsáno podrobněji.

PŘIDÁNÍ VLASTNÍCH SPOJENÍ

Vlastní relace jsou v obecném případě dvojího druhu: buď připojení k serveru a zobrazování celého desktopu (plochy) nebo pouze spuštění publikované aplikace. Nové relace se vytvářejí u Windows klienta poklepáním na ikonu Add ICA Connection, u unixového klienta pak volbou z menu Entry → New...

Pro potřeby OrionTS-IS jsou k dispozici pouze publikované aplikace – LEGSYS, MAGION a STAG. Pro každou z uvedených aplikací je třeba udělat samostatné spojení ("ikonku"). Při přidávání nových spojení je třeba nastavit:

- Typ spojení na `LAN (Local Area Network)`.
- Připojení nastavit na `Published Application`, a vybrat konkrétně aplikaci: LEGSYS, MAGION, nebo STAG (mělo by jít vybrat ze seznamu).
- Zobrazení v `Remote Desktop Window`, tj. nikoli `Seamless Window` (!).
- V případě, že z daného stroje bude k TS přistupovat jen jeden člověk, lze předvyplnit jeho jméno.
- V dalším okně lze upravit nastavení barev a rozlišení – obvykle necháváme standardní.

Ve Windows všechny tři ikony přidáme do nabídky Start do podmenu Citrix ICA Client, případně také přímo na plochu. Každou publikovanou aplikaci je dobré zkusit alespoň jednou spustit. Může se stát, zvlášť pokud uživatel pracuje standardně v rozlišení 800 × 600, že se aplikace STAG zobrazuje s posuvnými lištami, aby se na obrazovku vešla. Toto lze obejít tak, že v příslušných vlastnostech pro tuto publikovanou aplikaci (STAG) změníme Window Size na Full Screen.

POUŽITÍ ICA KLIENTA

Po spuštění jednotlivých aplikací se klient připojí k terminálovému serveru a za chvíli se vám objeví okno spouštěné aplikace. Zkontrolujte, zda se připojujete do domény `ZCU.CZ (Kerberos Realm)`, v opačném případě tuto variantu vyberte. Pokud řádka *Log on to:* chybí, klikněte na tlačítko Options a ona se objeví.

! Co dělat při problémech? Nejdůležitější je problém kvalifikovaně nahlásit, nejlépe standardní cestou operátorské službě CIV. V tomto případě zejména prosím nezapomeňte zřetelně uvést, že pracujete se službou tenkého klienta.

! Ukončování aplikací: Pouhé uzavření okna kolem aplikace neukončuje její chod. Aplikace běží dál a při novém připojení ke službě se uživatel dostane do stavu ve kterém zavřel okno (totéž platí, pokud bylo přerušeno spojení na server). Při ukončování práce je však potřeba aplikaci uzavřít (z menu aplikace), neboť pravidelná noční aktualizace by mohla narušit rozpracovanou činnost.

3.5 ZÁKLADNÍ SLUŽBY ORION

Projekt ORION je distribuované výpočetní prostředí poskytující hlavní služby udržované v rámci ZČU centrálně (CIV) a dostupné všem studentům a zaměstnancům. Kromě výše uvedených služeb, tvoří jádro ORIONu služba jednotné autentizace a sdíleného diskového prostoru.

3.5.1 JEDNOTNÁ AUTENTIZACE

Základní služba výpočetního prostředí garantující jednotný mechanismus prokázání identity uživatele. Elektronická identita je zjednodušeně řečeno uživatelské konto. Uživatelské jméno vás jednoznačně identifikuje vůči všem službám i ostatním uživatelům. Heslo slouží jako důkaz příslušnosti k této vaší (elektronické) identitě.

K přístupu ke všem službám používá uživatel tutéž identitu, přičemž ve většině případů se prokázání identity vůči konkrétní službě děje pro něj zcela transparentně na základě toho, že prokázal svoji identitu při vstupu do výpočetního prostředí (zpravidla přihlášení na pracovní stanici).

Použitá technologie (Kerberos) dovoluje poskytování služby centrální autentizace (důvěryhodného prokázání elektronické identity) dalším službám a aplikacím, proto se uživatel setkává s touto základní službou (ač většinou nevědomě) na mnoha místech (menza, katedrální výpočetní prostředí, apod.). Neškodí na tomto místě zopakovat, že v rámci ZČU je tato identita jednou ze základních věcí (podobně jako výkaz studenta či karta JIS (průkaz studenta)) na kterou je třeba dbát a chránit ji jako své důležité soukromé vlastnictví.

Ve vašem operačním systému lze použít Kerberos pro autentizaci uživatelů při přihlášení nebo alespoň jako možnost transparentní práce s aplikacemi, které Kerberos podporují (uživatel se přihlásí lokálně a následně získá Kerberos identitu v rámci svojí pracovní relace).

Nastavení obvykle najdete v konfiguračním souboru `krb5.conf`. Konkrétní parametry Kerberos realmu ZČU jsou uvedeny v následující tabulce.

Kerberos realm	ZCU.CZ
Kerberos verze	5
Kerberos server (KDC)	kerberos1.zcu.cz
Alternativní KDC	kerberos2.zcu.cz
Alternativní KDC	kerberos3.zcu.cz
Kerberos admin server	kerberos-adm.zcu.cz

SLUŽBA PŘESNÉHO ČASU

Jednou z podmínek pro použití služby jednotné autentizace je udržování času pracovní stanice v předepsané maximální odchylce od přesného času (chyba pod 2 minuty). Přesný čas na pracovní stanici i katedrálních či fakultních serverech lze automatizovaně udržovat službou přesného času. Stačí nainstalovat příslušný software realizující protokol NTP a nakonfigurovat ho dle následující tabulky.

Protokol časové služby	NTP
Časové servery	clock1.zcu.cz, clock2.zcu.cz

Udržovat přesný čas doporučujeme i na všech stanicích a serverech, které služby ORIONu nepoužívají. Pro správné zobrazení času je nezbytné odpovídající nastavení časové zóny na koncové stanici (správné nastavení časové zóny zařídí i automatické přepnutí letního času).

SLUŽBA KX.509 – POUŽITÍ JEDNOTNÉ AUTENTIZACE PRO WWW

Technologie Kerbera není podporována ve světě WWW aplikací. V rámci ORIONu je pro transparentní použití jednotné autentizace pro WWW aplikace k dispozici služba KX.509, která je technologicky založena na konverzi „průkazu identity“ do dočasných certifikátů dle X.509. Aby uživatelé mohli na

stanici použít této služby, musí mít k dispozici klientské programové vybavení s příslušnou konfigurací. Služba KX.509 je ve zkušebním provozu a její instalace není zatím nezbytná pro běžnou práci uživatelů.

3.5.2 SDÍLENÝ DISKOVÝ PROSTOR

V rámci projektu ORION má každý uživatel přidělen svůj diskový prostor (domovský adresář) pro ukládání dat. Tento prostor je určen primárně pro úschovu důležitých dat uživatele, může však také sloužit k jejich sdílení mezi více uživateli (přístup k datům řídí každý vlastník dle svých potřeb). Dále pak může uživatel nebo skupina uživatelů získat další diskový prostor (nazývaný projekt) pro rozsáhlejší práci.

Službu diskového prostoru technicky zabezpečuje distribuovaný souborový systém AFS. Instalace i konfigurace klienta je záležitost výhradně správce stanice, uživatel nastavuje přístupová práva ke konkrétním datovým oblastem. Pro přístup k chráněným částem souborového systému se používá autentizační služba Kerberos.

Jestliže ve svém operačním systému nemáte k dispozici AFS, tak si stáhněte instalační balík klienta AFS z projektu OPEN ORION nebo z `http://www.openafs.org`. Základní parametry AFS buňky ZČU najdete v následující tabulce.

AFS buňka (cell name)	zcu.cz
AFS DB servery	oknos.zcu.cz, nic.zcu.cz, sauron.zcu.cz

3.5.3 UŽIVATELSKÉ SERVERY ANEB TERMINÁLOVÝ PŘÍSTUP

Všichni uživatelé mají k dispozici pro svoji práci uživatelské servery, kde mohou vzdáleně pracovat prostřednictvím terminálového přístupu, navíc mohou jejich prostřednictvím přenášet soubory vně či dovnitř ORIONu. K terminálovému přístupu resp. přenosu souborů je potřeba instalovat programové vybavení schopné realizovat příslušné zabezpečené komunikační protokoly. Vlastní konfigurace se již zpravidla provádí na úrovni uživatele.

Podrobnější informace včetně konkrétních odkazů na doporučované programové vybavení a návodů na jeho použití naleznete ve sborníku CIV 3/2003 kapitola 4 a na `http://support.zcu.cz`. Zde pouze základní fakta.

SOFTWARE PRO TERMINÁLOVÝ PŘÍSTUP

Pro terminálový přístup k uživatelským serverům je třeba použít aplikace s podporou protokolu SSH v2. V unixových distribucích je takový software běžnou součástí (ssh), do MS Windows je třeba doinstalovat některý z dostupných SW balíků. Doporučovaným je `PuTTY`.

SOFTWARE PRO PŘENOS SOUBORŮ

Situace u přenosu souborů je podobná. Přístup je možný pouze protokoly z rodiny SSH (FTP není podporováno), čili opět v unixovém světě jsou aplikace jako `scp` běžně k dispozici, do MS Windows je třeba je doinstalovat. Implementací scp pro Windows je program `pscp` z rodiny `PuTTY`.

! Pro přístup k datům na sdíleném souborovém systému lze s řadou výhod oproti použití aplikace pro přenos souborů doporučit instalaci AFS klienta (popis viz výše).

3.5.4 UŽIVATELSKÉ ÚČTY A JEJICH PARAMETRY

Pro kompletní nasazení služeb OPEN ORIONu je zde i služba dovolující automatickou propagaci uživatelských účtů na koncovou stanici. Tato služba je koncipována hlavně pro nasazení typu „katedrální učebna“, nicméně její součástí je i možnost omezení skupiny uživatelů, kteří se mohou na dané stanici

přihlásit. Součástí služby je distribuce centrálně udržovaných skupin, lze definovat i skupiny vlastní a tyto použít pro omezení přístupových práv ke stanici.

Služba využívá funkcionality NSS (*Name Service Switch*) resp. modulu NSS_LDAP koncového OS a publikuje data o uživatelských kontech protokolem LDAP dle RFC2307. Tento postup doporučujeme použít v OS typu UNIX, pro MS Windows máme k dispozici službu pracující s Active Directory – viz kap. 3.6.

Základní technické údaje jsou shrnuty v následující tabulce, podrobné informace viz uživatelská dokumentace LDAP služby (projekt Pleiades).

LDAP server (hostname)	ldap.zcu.cz
báze dat (base DN)	ou=rfc2307,o=zcu,c=cz
autentizace	anonymní přístup
verze LDAP protokolu	2 i 3
zabezpečení SSL	ne (port 389)

! Novou službou, určenou zejména pro nasazení OPEN ORIONu ve smyslu „katedrální učebna“, je služba omezení přihlášení na stanici dle JIS (jednotný autentizační systém). Tato služba umožní omezení přihlašovaní na stanici pouze těm uživatelům, kteří jsou dle JIS aktuálně v místnosti (laboratoři). Navíc se tak transparentně použije přístupový seznam studentů do laboratoře, který je třeba v systému JIS stejně udržovat kvůli řízení vstupů. Služba je realizována formou přídavného autorizačního modulu od OS a je v současné době na začátku ověřovacího provozu.

3.6 INFRASTRUKTURA DOMÉNOVÝCH SLUŽEB PRO MS WINDOWS

CIV poskytuje rozšířené služby, které umožňují napojení služeb Active Directory podporovaných serverovými systémy Windows 2000 Server a Windows 2003 Server na infrastrukturu prostředí ORION. K propojení obou světů slouží doména Active Directory s názvem `W2K.ZCU.CZ`. Ta je kořenem stromu domén, které mohou jejím prostřednictvím přistupovat k centrálním službám.

Služba je určena pracovištím, která chtějí provozovat vlastní stanice s OS Windows[5], ale zároveň chtějí v maximální možné míře využívat výhody nabízené prostředím ORION – především jednotné uživatelské základny a s tím spojených služeb (SSO přístup k dalším zdrojům). Pracoviště, které uvažuje o vytvoření své vlastní domény Active Directory na bázi serveru s OS Windows 2000/2003, má možnost zařadit tuto doménu do stávajícího stromu domén, v němž je zajištěna automatická údržba uživatelských účtů, skupin, případně dalších informací.

3.6.1 PRINCIP FUNGOVÁNÍ

Základní myšlenka již byla popsána výše a prostor vyhrazený tomuto článku nedostačuje pro širší popis, proto uvedeme jen stručný přehled v bodech. Co tedy připojení do infrastruktury domén Active Directory znamená:

- Pracoviště provozuje svůj vlastní server MS Windows 2000 (resp. 2003) jako řadič své vlastní domény. Pro ilustraci si zaveďme fiktivní doménu s názvem `katedra`.
- Doména není samostatná – je součástí doménového stromu `W2K.ZCU.CZ`. Její úplný název tedy zní `katedra.W2K.ZCU.CZ`.
- Mezi doménou `katedra` a top-level doménou `W2K` existuje vztah důvěry. Správce domény `katedra` proto může přistupovat k objektům zavedeným v doméně `W2K`. V ní se udržují nejen informace o všech uživatelských účtech existujících v prostředí ORION, ale také o centrálně aktualizovaných skupinách (studenti, zaměstnanci, skupiny vytvořené podle příslušnosti k fakultám apod.)

[5] Ke službě Active Directory mohou přistupovat stanice s Windows 2000 a následnými verzemi – vždy alespoň ve verzi Professional (v distribucích Home se služba AD nepodporuje).

- Doména `katedra` při tom zůstává plně pod kontrolou svého správce. Místní správce může vytvářet další uživatelské účty a skupiny platné v jeho doméně, definovat vlastní politiky a libovolně využívat další možnosti, které mu koncept Active Directory nabízí.
- Změny, které je třeba provést na lokálních stanicích, jsou minimální a lze je velmi snadno automatizovat.
- Na stanicích, které jsou součástí domény (např. naší vzorové domény `katedra`), lze snadno zprovoznit software pro přístup k dalším službám poskytovaným v prostředí ORION [6]:
  - Přihlašování pomocí jednotného uživatelského jména a hesla.
  - SSO přístup k centrálnímu souborovému systému AFS.
  - Při použití vhodného klienta i SSO přístup k elektronické poště.
  - SSO přístup k centrálním aplikačním serverům (`eryx`, `satyr...`).
  - SSO vydávání krátkodobých certifikátů pro přístup k webovým aplikacím (KX509).

3.6.2 POSTUP AKTIVACE SLUŽBY

Zařazení vaší domény do stromu `W2K.ZCU.CZ` vyžaduje spolupráci pracovníků CIVu – z bezpečnostních důvodů není možné připojovat do tohoto stromu subdomény bez patřičného oprávnění. Chcete-li této služby využít, kontaktujte CIV obvyklým způsobem – nejlépe e-mailem na `operator@service.zcu.cz`. Pracovník CIV si s vámi domluví schůzku, zodpoví případné dotazy a bude vám asistovat při instalaci služby.

Na návštěvu pracovníka CIV a instalaci služby se můžete připravit předem. Budete potřebovat: server s OS Windows 2000 Server (resp. 2003 Server)[7], alespoň jednu vzorovou stanici s OS Windows 2000 Professional nebo Windows XP Professional a asi 2 hodiny času. S případnými dotazy se obracejte standardní cestou na uživatelskou podporu CIV.

3.7 DALŠÍ SLUŽBY

3.7.1 SDÍLENÝ KALENDÁŘ ANEB GROUPWARE LOTUS NOTES/DOMINO

Systém Lotus Notes/Domino (LN) reprezentuje komplexní softwarové řešení (platformu) zaměřené na podporu spolupráce a komunikace v rámci pracovních týmů (tzv. groupware). Poskytované nástroje umožňují efektivní organizaci a plánování času, řízený oběh dokumentů a jejich sdílení, rezervaci místností a dalších zdrojů, zřizování a správu diskusních fór či skupin apod. Standardní součástí systému jsou i vývojové nástroje umožňující relativně snadnou a rychlou úpravu existujících a vývoj nových aplikací (LN databází).

Technologicky jsou LN koncipovány jako distribuovaný a multiplatformní systém na bázi architektury klient/server, jehož jádro tvoří vyspělý e-mailový subsystém podporující všechny běžně využívané standardy. Velký důraz je kladen na bezpečnost (integrální součástí veškeré komunikace je zabezpečení pomocí asymetrické šifry), podporu práce off-line, snadnou škálovatelnost a vysokou dostupnost.

SLUŽBA LN A JEJÍ POSKYTOVÁNÍ

Systém LN je v různé formě provozován v rámci služeb CIV déle než rok. V současnosti jej rutinně využívá více než 150 uživatelů z řad zaměstnanců i externích spolupracovníků. Na platformě LN je založen též e-learningový systém EDEN používaný na ZČU.

[6] Pro další informace viz také další části tohoto sborníku.
[7] Vhodné je mít k dispozici také instalační CD systému.

CIV provozuje 2 servery LN/Domino 6.x na OS Debian/Linux. Přístup je podporován jak z nativních klientů LN (existují pouze pro MS Windows NT SP6 a vyšší), tak přes WWW prostřednictvím Domino Web Access (prohlížeče MSIE 5.5 a Mozilla 1.3.1 a vyšší s podporou Javy).

Aktuálně CIV poskytuje LN jako doplňkovou (tj. standardně nenárokovatelnou) službu pro zaměstnance (resp. zaměstnanecké kolektivy), jejíž podpora je řízena podle strategie „best effort“. Součástí služby může být zřízení konta, instalace a konfigurace klientského SW, základní uživatelské školení, zřizování (příp. modifikace) týmových LN databází, rutinní zálohování a standardní podpora řešení uživatelských problémů prostřednictvím RT systému. Konkrétní specifikace finanční náročnosti, úrovně technických podmínek a podpory bude individuálně upřesněna s každým zájemcem. O podmínkách a poskytnutí služby rozhoduje v konečné instanci vedení CIV.

Podrobnější informace o systému LN a poskytování této služby lze získat standardním způsobem prostřednictvím služby HelpDesk (`operator@service.zcu.cz`, RT fronta `notes`).

KONCEPCE DALŠÍHO ROZVOJE

Platforma LN je z pohledu CIV perspektivním řešením s dostatečným potenciálem, které bude i nadále podporováno. CIV se podílí na řešení několika projektů komponent IS v rámci projektu e-univerzity využívajících jejích integračních vlastností. Uvažujeme také o zpřístupnění rozvinutých kolaborativních nástrojů (team workplace) pro potřeby výuky a studentských kolektivů (kroužků a pracovních skupin). Souběžně s budováním univerzitního portálu a přechodu na J2EE technologie bude probíhat také integrace platformy LN.

3.7.2 VIRTUÁLNÍ WEBY ANEB WEBHOSTING

CIV již několik let poskytuje službu virtuálních WWW serverů (webhosting), která je nejčastěji využívána pro provoz katedrálních stránek a prezentaci jednorázových akcí (například konference), ale lze ji samozřejmě nasadit i pro jiné účely. Služba je v rutinním provozu, poskytuje již více než 130 registrovaných WWW virtuálních serverů.

Chce-li například katedra vystavit své WWW stránky, má několik možností. Jedním řešením může být nasazení vlastního WWW serveru, ale to je ovšem spojeno s několika problémy: Je nutné zakoupit nebo vyčlenit hardware, pořídit patřičný software pro provoz WWW serveru, zajistit kvalifikovaného správce stroje i webserveru a určit pracovníka, který se bude starat o informace publikované na těchto stránkách. Nezbytností je také zálohování dat (kvůli poruchám HW a útokům hackerů).

Druhým řešením – méně náročným na zdroje – je využít službu provozu virtuálních WWW serverů poskytovanou CIV. Tato služba provozována na dostatečně výkonném stroji dokáže bezproblémově hostovat i několik set WWW virtuálních serverů. Data jednotlivých virtuálních WWW serverů jsou na AFS (jako tzv. projekty) a správce stránek k nim má zajištěn bezproblémový přístup např. ze své stanice (nejčastěji Windows s OpenAFS klientem) nebo vzdáleně po přihlášení na server eryx (ssh, WinSCP, apod.).

Výhod pro koncového uživatele má řešení prostřednictvím virtuálního WWW serveru hned několik:

- nulové náklady na HW, správu OS a WWW serveru,
- zálohování dat (projektu) 1x týdně a zabezpečení serveru proti neoprávněnému přístupu,
- přístup k datům pro správce obsahu prakticky odkudkoli.

Jak toto všechno získat? Velmi jednoduše – stačí vyplnit formulář pro zřízení projektu virtuálního WWW serveru, který naleznete na URL `http://www.projekt.zcu.cz/`

KAPITOLA 4

OPEN ORION PRO DEBIAN LINUX

V rámci projektu OPEN ORION vznikl soubor balíčků pro platformu Debian Linux. Jejich instalací si můžete zajistit přístup k jednotlivým službám nabízeným prostředím ORION.

4.1 PŘEDPOKLADY PRO INSTALACI

Projekt OPEN ORION předpokládá nainstalovanou a řádně nastavenou stanici s připojením do sítě WEBnet. Pro provedení instalace se vyžaduje administrátorský přístup a alespoň minimální znalosti správy linuxové stanice. Samozřejmostí je konto v síti WEBnet a HTTP přístup ke zdroji s instalačními balíčky.

V současné fázi projektu je možno použití OPEN ORION balíčků pouze pro distribuci Debian. Pro ostatní distribuce jsou k dispozici informace potřebné pro instalaci *manuální* cestou, základní údaje o poskytovaných službách a jejich konfiguraci jsou shrnuty v kap. 3. Navíc existuje starší podrobný popis jak orionizovat stanici s distribucí RedHat. Popis je možné najít na adrese:
`http://support.zcu.cz/prostredi/OpenOrionRH7.html`

4.2 DISTRIBUCE DEBIAN, SPRÁVA SW BALÍČKŮ

Projekt OPEN ORION přináší uživatelům Linuxu v distribuci Debian sadu balíčků, jež využívají příslušné prvky této distribuce. Také řeší jejich případné závislosti a provedou základní konfiguraci pro prostředí ORION.

4.2.1 DPKG, APT

Poskytované balíčky jsou udržovány ve formátu pro manažer DPKG. Soubory jsou dostupné na adrese `http://openorion.zcu.cz/debian/` nebo `http://support.zcu.cz/download/OpenOrionLinux/`

Balíčky jsou provázány závislostmi s balíčky standardní distribuce a instalují příslušné konfigurační soubory pro prostředí ORION.

4.2.2 KONFIGURACE APT

Pro instalaci balíčků se doporučuje použít instalační metodu `apt` (Advanced Package Tool). Nastavení `apt` se provede přidáním následujícího řádku do konfiguračního souboru `/etc/apt/sources.list`:

```
deb http://openorion.zcu.cz/debian unstable main
```

Dále je vhodné provést příkaz `apt-get update`, aby se načetl seznam nových balíků.

4.2.3 DOTAZY PŘI INSTALACI

Balíčky OPEN ORIONu závisí na standardních balících z distribuce Debian, a proto se při jejich instalaci program `dpkg` ptá na potřebná konfigurační nastavení. Ale všechny orionizované balíky se sami postarají o konfiguraci jednotlivých služeb a není třeba na dotazy `dpkg` reagovat (např. parametry Kerbera, jména časových serverů, apod.) – stačí je jenom „odklepat“.

Pokud nechcete zbytečně odpovídat na konfigurační dotazy balíků, které závisí na orionovských, je možné na dobu instalace překonfigurovat balík *debconf* příkazem `dpkg-reconfigure debconf`, nastavit frontend jako `Noninteractive` a prioritu dotazů na `Critical`. Po instalaci je možné stejným příkazem nastavit `debconf` na původní hodnoty.

4.3 POSKYTOVANÉ SLUŽBY A JIM ODPOVÍDAJÍCÍ BALÍČKY

Základní služby implementované balíčky odpovídají popisu služeb v kap. 3.

Autentizace Nakonfiguruje stanici jako klienta pro službu jednotné autentizace protokolem Kerberos5 (balíček *krb5orion*). Dále je k dispozici balíček zajišťující instalaci a konfiguraci správných nástrojů pro terminálový přístup a přenos souborů protokolem SSH (*sshkrb5orion*), a v ověřovacím provozu také klient pro transparentní použití jednotné autentizační služby pro WWW aplikace (*kx509orion*).

Souborový systém Přístup uživatele ke sdílenému souborovému systému. Více viz kap. 3.5.2. SW balík s implementací OpenAFS klienta je standardně k dispozici v distribuci Debian, jeho část se však musí zkompilovat. Balíček *openafsorion* závisí na tomto standardním balíku, dodává k němu konfiguraci služby ORION a podrobnou dokumentaci ke kompilaci a instalaci. Protože je tato činnost poněkud složitá, poskytuje projekt OPEN ORION zkompilované moduly OpenAFS pro standartní verze linuxového jádra z distribuce Debian, *openafs-modules2*.

Zabezpečení stanice proti napadení Doporučený balík zajišťující ochranu počítače na bázi osobního firewallu — balíček *fireorion*. Používá standardní vlastnosti distribuce Debian, obsahuje konfiguraci v souladu s doporučeními CIV pro ochranu stanice (viz kap. 2).

Pošta Přístup k osobní poštovní schránce pomocí standardních klientů. Realizováno pomocí `pine`, IMAP4 s využitím autentizace Kerberos5 – balíček *pineorion*

Tiskové služby Nastavení sdílených tiskáren v prostředí ORION. — balíček *printorion* — nezávisí na žádné jiné službě a slouží k automatizovanému nastavení tiskových front (popsaných v kap. 3.3) na stanici.

Jednotlivé služby je možno aktivovat nainstalováním příslušného balíku. K aktivaci všech dostupných služeb slouží balíček *orion*. K výše zmíněným balíčkům patří ještě *ntporion, ldaporion* a *pamorion*, které zajišťují podpůrné funkce.

4.4 ZÁKLADNÍ VARIANTY NASAZENÍ

Existuje několik základních scénářů jak OPEN ORION použít. Instalační balíčky napomáhají tvorbě vhodných kombinací tím, že na sobě závisí logicky dle závislostí jednotlivých služeb (např. instalace klienta souborového systému automaticky vynutí instalaci autentizační služby).

- **Systém se základními přístupovými prostředky**
  Po instalaci budete mít na své stanici k dispozici nástroje prostředí ORION pro autentizaci (`kinit, klist, kdestroy`). Po prvotním ověření (`kinit`) může uživatel přistupovat přímo ze své stanice bez další autentizace na veřejné unixové servery sítě WEBnet (`ssh` a `scp`, tj. terminálový přístup i přenos souborů) a k poště klientem Pine.

Použijte balíčky *krb5orion, sshkrb5orion a pineorion*. Doporučujeme použít i balíček *fireorion* pro ochranu stanice osobním firewallem a balíček *openafsorion* (`aklog, unlog` pro přístup do sdíleného diskového prostoru AFS. Můžete také použít *printorion*, pokud chcete používat tiskové služby.

- **Systém s ORION klientem**
  Použijte zastřešující balíček *orion*. Funkcionalita viz výše, každý uživatel má po autentizaci k dispozici přímo přístupné svoje nebo sdílené diskové prostory na AFS (domovský adresář a projekty), ke kterým může přistupovat ze všech strojů s AFS klientem.

  Lokální uživatelská konta jsou přes *pam*-moduly napojena na centrální autentizační službu (nebudete muset řešit zapomenutí hesel uživatelů). Pouze vytvořte uživatelská konta se stejným uživatelským jménem jako uživatele mají v ORIONu a řekněte jim, že se ke stanici mají hlásit svým heslem z ORIONu. Navíc takto uživatel získá pověření (elektronickou identitu) při přihlášení na stanici a nemusí dělat příkaz `kinit` (může rovnou přistupovat na AFS apod). Více v dokumentaci na `http://support.zcu.cz/prostredi/OpenOrionLinux.html`

- **Stanice do učebny**
  K výše uvedenému přidejte službu distribuce centrálně udržovaných uživatelských účtů a jejich vlastností balíčkem *ldaporion*. Jak bylo popsáno v kap. 3.5.4 (a podrobný návod najdete v dokumentaci balíčku *ldaporion*), máte možnost omezit přihlašování uživatelů na vaše stanice na základě centrálně i lokálně udržovaných skupin. A nemusíte zakládat konta na stanicích. Stačí se postarat o odpovídající aplikační programové vybavení.

4.5 POPIS INSTALAČNÍCH BALÍČKŮ

orion Zastřešující balík, který obsahuje závislosti na ostatní orionizované balíky. Pokud nainstalujete tento balík, vyřeší instalaci ostatních za Vás. Obsahuje též instalační dokumentaci (`http://openorion.zcu.cz`) Po instalaci je potřeba dokonfigurovat a dokompilovat moduly pro OpenAFS (viz. níže)

Instalace: `apt-get install orion`

krb5orion Balík obsahuje instalaci a konfiguraci autentizačního systému Kerberos5 `/etc/krb5.conf` v prostředí ORION, který zajišťuje bezpečnostní ověřování uživatelů.

Instalace: `apt-get install krb5orion`

sshkrb5orion Balíček pro instalaci SSH, systému pro bezpečné vzdálené přihlášení. Nainstaluje potřebné balíky (`ssh-krb5`, ...) a nakonfiguruje ssh démona a klienta pro autentizaci vůči Kerberu5 včetně pam modulů. Konfigurační soubory: `/etc/ssh/ssh_config`, `/etc/pam.d/login` a `/etc/pam.d/ssh`

Instalace: `apt-get install sshkrb5orion`

openafsorion Balíček pro zpřístupnění distribuovaného souborového systému OpenAFS. S jeho pomocí může uživatel přistupovat ke sdílenému diskovému prostoru. Obsahuje konfiguraci a zdrojové soubory OpenAFS modulů pro Linuxové jádro. Ty je potřeba následně přeložit. Více v dokumentaci obsažené v balíku (`/usr/share/doc/openafsorion/INSTALL.openafsorion.html`) nebo na webu:
`http://support.zcu.cz/prostredi/OpenOrionLinux/INSTALL.openafsorion.html`.

Instalace: `apt-get install openafsorion`

openafs-modules2 Virtuální balík s předkompilovanými moduly pro vybraná jádra řady 2.4. Při instalaci zobrazí jména skutečných balíků, které je možno instalovat, z nich uživatel vybere balík příslušný k jádru jež používá. Více v dokumentaci balíku *openafsorion*.

ntporion Balíček pro nainstalování a nakonfigurování (`/etc/ntp.conf`) služby pro automatickou synchronizaci hodin v počítači s lokálními časovými servery. Tato služba je nezbytná pro správné fungování autentizace Kerberos5.

Instalace: `apt-get install ntporion`

pineorion Balíček poštovního klienta. Obsahuje orionizovaný Pine s podporou pro Kerberos5, SSL, IMAP a LDAP. Dodává do systému samotný program Pine a skripty pro vytvoření lokálního konfiguračního souboru, včetně zaregistrování do systému tak, aby se nechal spustit jednoduše příkazem `pine`.

Instalace: `apt-get install pineorion`

ldaporion Balíček zajistí propojení lokálních databází kont (`/etc/passwd`) s LDAP serverem. Tím lze umožnit autorizaci a přihlášení uživatele, který nemá na daném stroji lokální konto. Taktéž poskytuje řízení přístupu uživatelů na daný stroj podle uživatelského jména nebo členství ve skupinách. Více v dokumentaci obsažené v balíku (`/usr/share/doc/ldaporion/README.ldaporion.html`) nebo na webu: `http://support.zcu.cz/prostredi/OpenOrionLinux/README.ldaporion.html`.

Tento balík není instalován automaticky s balíčkem *orion*.

Instalace: `apt-get install ldaporion`

pamorion Balíček obsahující konfiguraci PAM modulů pro všechny služby OPEN ORIONu.

Tento balíček se instaluje a konfiguruje automaticky podle závislostí na ostatních balíčcích.

Instalace: `apt-get install pamorion`

printorion Balík nakonfiguruje sdílené tiskárny poskytované prostředím ORION. (`/etc/printcap`)

Instalace: `apt-get install printorion`

kx509orion Balík pro instalaci knihoven pro práci s krátkodobými certifikáty vydanými na základě Kerberos identity v prostředí ORION.

Více v dokumentaci obsažené v balíku (`/usr/share/doc/kx509orion/INSTALL.kx509orion.html`) nebo na webu: `http://support.zcu.cz/prostredi/OpenOrionLinux/INSTALL.kx509orion.html`.

Instalace: `apt-get install kx509orion`

fireorion Balík konfigurující osobní firewall z linuxového jádra (Netfilter.org).

Jak přeložit jádro s potřebnými funkcemi a moduly naleznete v dokumentaci obsažené v balíku (`/usr/share/doc/fireorion/README.fireorion.html`) nebo na webu: `http://support.zcu.cz/prostredi/OpenOrionLinux/README.fireorion.html`.

Instalace: `apt-get install fireorion`

4.6 DODATKY

Některé konfigurační soubory pro výpočetní prostředí ZČU a další spřátelené sítě jsou v aktuální verzi na AFS v adresáři `/afs/zcu.cz/common/etc`, odkud si je lze zkopírovat pro vlastní úpravy.

Další užitečné informace naleznete na stránkách `http://support.zcu.cz/openorionlinux` nebo `http://openorion.zcu.cz` nebo následujte webové odkazy v dokumentaci k jednotlivým balíčkům.

KAPITOLA 5

OPEN ORION PRO WINDOWS

V rámci projektu OPEN ORION vznikl také soubor balíčků pro platformu MS Windows. Jejich instalací si můžete zajistit přístup k jednotlivým službám nabízeným prostředím Orion. Žádný z balíčků není mandatorní, ale jisté závislosti přesto existují (na úrovni doporučení). Závislosti jsou popsány individuálně u každého balíčku.

5.1 OPEN ORIONT VERSUS OPEN ORIONXP

V dřívější době byl projekt OPEN ORION orientován na Windows NT (OPEN ORIONT). V průběhu roku 2004 postupně končí podpora Windows NT a nastává přechod na Windows XP – to se týká zejména všech veřejných učeben CIV a počítačů IS (ORIONT–IS).

V souvislosti s touto změnou byl ukončen veškerý vývoj pro Windows NT a od jara 2004 jsou k dispozici balíčky pro Windows XP (OPEN ORIONXP).

Poznámka: Instalační balíčky pro OPEN ORIONXP lze až na některé výjimky[1] používat též v systému Windows 2000.

5.2 INSTALACE BALÍČKŮ

Softwarové balíčky pro OPEN ORIONXP nainstalujete spuštěním programů, které získáte na adrese `http://support.zcu.cz/openorionxp` Na uvedené stránce rovněž naleznete podrobné návody na instalaci.

5.3 POPIS BALÍČKŮ

Kerberos Balíček Kerberos představuje – zjednodušeně řečeno – jádro distribuce OPEN ORION na vašem počítači. Obsahuje implementaci základních prostředků ověřovacího systému Kerberos na platformu Microsoft Windows.

Balíček Kerberos nevyžaduje instalaci. Soubory uložené v archivu stačí rozbalit do libovolného adresáře. Chcete-li nástroje balíčku Kerberos využívat pravidelně, můžete na svém systému ještě upravit systémovou proměnnou `PATH` tak, aby se spustitelné soubory Kerbera daly volat odkudkoli.

Balíček není závislý na žádném dalším balíčku sady OPEN ORION.

Dokumentace: `http://support.zcu.cz/prostredi/OpenOrionXP/kerberos.html`

[1] například automatická instalace tiskáren

? Mohu použít balíček Kerberos i pro přihlášení ke svému počítači?

Chcete-li se ke svému počítači přihlašovat s identitou, která vám byla přidělena v prostředí ORION, nebude vám balíček Kerberos stačit. Používáte-li systém Windows NT, můžete použít knihovnu Gina Light – viz `http://openorion.zcu.cz`. Řešení pro systémy Windows 2000 a Windows XP vyžaduje zařazení vašeho pracoviště do stromu domén Active Directory – viz kap. 3.6.

AFS Klient Klient souborového systému AFS vám umožní přístup k datům uloženým v centrálním diskovém prostoru (domovské adresáře uživatelů, projekty, webový prostor). Na ZČU se v současnosti používá verze produkovaná pod označením OpenAFS. Instalační balíček můžete získat ze stránek projektu OPEN ORION, nebo přímo z distribučních stránek `www.openafs.org`.

Při instalaci bude třeba zadat několik parametrů. Průběh instalace je podrobně popsán na zmíněné webové stránce – na tomto místě uvedeme jen přehled potřebných informací:

Nejdůležitější je poskytnout klientu informace o *buňce AFS* (*AFS Cell*). Název buňky nastavte na `zcu.cz` a jako databázové servery uveďte `nic.zcu.cz`, `oknos.zcu.cz` a `sauron.zcu.cz` (viz také kap. 3.5.2). Po tomto nastavení bude možné klienta spustit a začít přistupovat k centrálnímu diskovému prostoru.

Doporučujeme nainstalovat také balíček *Kerberos*.

Dokumentace: `http://support.zcu.cz/prostredi/OpenOrionXP/afs_klient.html`

Wake Wake je grafická nadstavba, která vám umožňuje v jednotném prostředí ovládat funkce spojené se službami Kerberos a AFS. Wake umí získávat lístky a oprávnění pro přístup k AFS, vypisovat informace a ovládat mapování disků k prostoru AFS.

V grafickém rozhraní Wake mají uživatelé k dispozici tlačítka, jejichž funkce jsou ekvivalentní řádkovým příkazům balíčků Kerberos, AFS Klient a také některým řádkovým příkazům Windows (`ms2mit`, `kinit`, `aklog`, `net...`).

Instalace produktu Wake je velice jednoduchá. Při práci v prostředí ZČU se vás Wake může dotázat na název sféry Kerberos (*Kerberos Realm*) – **ZCU.CZ**. Může se vás dotázat také na název buňky AFS (*AFS Cell*) – i v tomto případě zadejte **zcu.cz**.

Doporučujeme nainstalovat také balíčky *Kerberos* a *AFSKlient*.

Dokumentace:`http://support.zcu.cz/prostredi/OpenOrionXP/Wake_dokumentace_cz.html`

Pine Pine je v prostředí počítačové sítě ZČU doporučeným klientem elektronické pošty. Jeho výhodou je, že je dostupný pro řadu platforem (UNIX, Linux, Windows) a bude se tedy líbit zvláště uživatelům, kteří často střídají pracovní prostředí.

Základní rozhraní klienta Pine je sice textové, ale funguje v něm velmi dobrá podpora prohlížečů nejrůznějších formátů a tak se dá pohodlně pracovat i s přílohami elektronické pošty.

Pine je v současnosti jediným poštovním klientem, který podporuje přímé ověření uživatele vůči systému Kerberos a proto jako jediný klient elektronické pošty nabízí v našem prostředí přístup SSO (single-sign-on).

Konfigurace klienta pro Windows není náročná. Chcete-li, můžete si stáhnout instalační balíček z adresy `http://support.zcu.cz/download/OrionXP/pcpine.exe`, rozbalit jej přímo do místa, ze kterého budete program spouštět, a zkonfigurovat skriptem `pineconf.bat`, který je součástí balíčku.

Doporučujeme nainstalovat také balíček *Kerberos*.

Dokumentace: `http://support.zcu.cz/prostredi/OpenOrionXP/pcpine.html`

Mozilla Thunderbird Program Mozilla Thunderbird doporučujeme jako grafického klienta pro práci s elektronickou poštou. V současnosti není k dispozici žádná verze upravená přímo pro práci v prostředí ORION. K instalaci tedy můžete použít nejen balíček dostupný na stránkách projektu OPEN ORION, ale i balíček stažený z jiných důvěryhodných zdrojů.

Mozilla Thunderbird nepodporuje ověření uživatele prostřednictvím normy Kerberos. Nejvýznamnějším důsledkem je to, že přístup k poště tímto klientem neumožňuje SSO[2] – vždy je třeba zadat své heslo, případně jej svěřit dostupným softwarovým prostředkům k zapamatování.

Instalace samotného produktu probíhá obvyklým způsobem. Při prvním spuštění se aplikace každého uživatele dotáže na konfigurační údaje. V prostředí ZČU platí tato nastavení (podrobněji viz kap. 3.2):

- *Adresa elektronické pošty* je adresa, kterou používáte na ZČU
- *Typ serveru pro příchozí poštu* je **IMAP**.
- *Příchozí server* (IMAP) je `imap.zcu.cz`, zabezpečení pomocí SSL zapnuto.
- *Odchozí server* (SMTP) je `smtp.zcu.cz`
- *Jméno uživatele* je vaše uživatelské jméno v systému ORION. Pokud jste správně vyplnili svoji adresu, bude již vaše jméno v konfiguraci napsáno.

Balíček není závislý na žádném dalším balíčku sady OPEN ORION.

Dokumentace: `http://www.czilla.cz/help/thunderbird/`

? Proč používat klient Mozilla Thunderbird?

Thunderbird nabízí prostředí, které je dobře známé uživatelům zvyklým na e-mailové klienty firmy Microsoft (Outlook nebo Outlook Express). Na rozdíl od nich však zaručuje větší bezpečnost při práci elektronickou poštou. Po několika vlnách rozsáhlých virových infekcí je nasazení tohoto klienta zajímavou alternativou pro ty, kdo se chtějí napříště vyhnout většině virů šířených elektronickou poštou.

? Umí Thunderbird pracovat s lokálními složkami na mém počítači?

Lokální složky, které na vašem počítači vytvořil jiný klient elektronické pošty (např. Outlook Express), nemůžete v klientu Mozilla Thunderbird používat přímo, ale můžete je převést do nového formátu. Práce s nimi je pak již bezproblémová.

Putty Putty je klient pro bezpečný terminálový přístup k serverům protokolem SSH2. Základní instalace je velice jednoduchá.

Klient Putty nám ovšem v prostředí ORION nabízí tu výhodu, že dokáže k ověření uživatele využívat Kerberos. Chcete-li získat SSO přístup k centrálním serverům projektu ORION (`eryx`, `satyr`...), nainstalujte si program putty, spusťte jej a konfiguraci upravte takto:

- V kategorii *Session* přepněte protokol na **SSH**.
- V kategorii *Connection* zadejte do okna *Auto-login username* své uživatelské jméno, které používáte v prostředí ORION.
- V kategorii *Connection/SSH* přepněte preferovanou verzi protokolu SSH na **2**. Ostatní volby můžete nechat neaktivní.
- V kategorii *Connection/SSH/Auth* musíte zaškrtnout volby *Attempt GSSAPI/Kerberos 5 authentication*, *Allow attempted changes of username in SSH2* a *Allow Kerberos 5 ticket forwarding*.
- Vhodné je také v kategorii *Connection/SSH/Tunnels* zapnout volbu *Enable X11 forwarding*.

[2] Single sign-on – uživatel zadá své identifikační údaje (jméno a heslo) pouze jednou při přihlášení a pak už pracuje se všemi zdroji bez nutnosti identifikaci opakovat.

Nastavení si můžete uložit jako implicitní (kategorie *Session* – položka *Default Settings*). Nastavení se ukládá pro každého uživatele zvlášť a zapisuje se do registru, takže nenastávají konflikty ani problémy s právy.

Pokud před spuštěním putty získáte lístek Kerberos (např. programem Wake nebo příkazem `kinit`), pokusí se putty při připojování k serveru SSH tento lístek použít a přihlásí vás bez nutnosti zadávat znovu heslo.

Doporučujeme nainstalovat také balíček *Kerberos*.

Dokumentace: `http://support.zcu.cz/prostredi/OpenOrionXP/putty.html`

Avast Avast je plnohodnotný antivirový program, který obsahuje nástroje pro kontrolu počítače na požádání, i nástroje pro rezidentní kontrolu zpracovávaných dat při běhu počítače (kontrola příchozí pošty, spouštěných aplikací apod.)

Avast je licencovaný software a Západočeská univerzita vlastní multilicenci, kterou pravidelně obnovuje. Instalace programu se tedy neobejde bez znalosti licenčního čísla.

K instalaci Avastu se dá použít instalační balíček dostupný na `http://support.zcu.cz/av/`, nebo jiný podporovaný zdroj.[3] V každém případě je však třeba uvedenou stránku navštívit, protože zde je uvedeno licenční číslo, bez nějž nelze provést plnohodnotnou instalaci.

Samotná instalace produktu probíhá standardním způsobem. K dispozici je i rozsáhlá nápověda. Doporučujeme vám, abyste s její pomocí nastavili svou instalaci Avastu pro automatickou aktualizaci virové databáze.

Balíček není závislý na žádném dalším balíčku sady OPEN ORION.

Dokumentace: `https://secweb.zcu.cz/avast/avast.html`

? Jak mám postupovat při vypršení platnosti licenčního kódu?

Nová licenční čísla publikujeme na stránce `https://secweb.zcu.cz/avast/avast.html`. K této stránce lze přistupovat pouze z počítačů umístěných na ZČU a vždy jen po zadání uživatelského jména a hesla. Licence je určena pouze pro použití na počítačích ZČU.

? Jaké verze Avastu můžeme používat? Jak je to se serverovou verzí?

Licenční číslo, které publikujeme na stránce `https://secweb.zcu.cz/avast/avast.html` platí pro verze Avast3 i Avast4. Můžete tedy používat tu, která je pro vás vhodnější. Máte-li zájem o instalaci serverové verze produktu, kontaktujte CIV.

? Potřebuji ještě další antivirový program?

Avast je plnohodnotným prostředkem ochrany proti počítačovým virům. V mezinárodně uznávaných testech dosahuje velmi dobrých výsledků. Používáte-li Avast, nepotřebujete jiný antivirový software.

? Proč neumí Avast léčit nakažené soubory?

Základním cílem antivirového programu je detekovat infekci a pokusit se jí zabránit. Pokud k nakažení dojde, je k dispozici celá řada nástrojů na odstranění viru. Výrobce Avastu poskytuje zdarma na svých stránkách `http://www.alwil.cz` produkt Avast Cleaner, který slouží k odstranění virů z infikovaných souborů.

Tiskové služby Instalaci tiskových služeb poskytovaných protokolem LPR a popsaných v kap. 3.3 pro vaši Windows stanici lze provést automatizovaně[4] instalačními balíčky, které jsou pro tento účel udržovány v rámci projektu OPEN ORION. Balíček pro libovolnou tiskárnu můžete stáhnout do

[3] Vždy nejnovější verzi Avastu můžete získat na webových stránkách výrobce – `http://www.alwil.cz`, nebo na distribučním CD. Instalační balíček připravený na stránce ZČU obsahuje parametrizovanou instalaci s předvyplněnými instalačními údaji.

[4] jen ve Windows XP

svého počítače z URL `http://support.zcu.cz/tisk/` a spustit instalaci. Proběhne automaticky vytvoření příslušného tiskového portu i instalace tiskárny.

Balíček není závislý na žádném dalším balíčku sady OPEN ORION.

Dokumentace: `http://support.zcu.cz/tisk/`

? Jaká je vazba tiskových služeb na prostředí ORION?

Informace uložené v ORIONu se používají k identifikaci uživatelů, kteří tiskové služby využívají. Budete-li tisknout z počítače bez patřičné identifikace (např. použijete-li pro tisk účet `root` nebo `administrator`), bude patrně vaše tisková úloha odmítnuta.

5.4 DALŠÍ INFORMACE

Aktualizované informace o všech balíčcích, které jsme v této kapitole zmínili, i o projektu OPEN ORION můžete najít na adrese `http://support.zcu.cz/openorionxp` a také `http://openorion.zcu.cz`

ISBN 80-7043-286-1