INFORMAČNÍ A ADMINISTRAČNÍ SYSTÉM

Pawouk 2010

# Seminář o bezpečnosti a anonymitě na Internetu

Radim Dolák

# Osnova

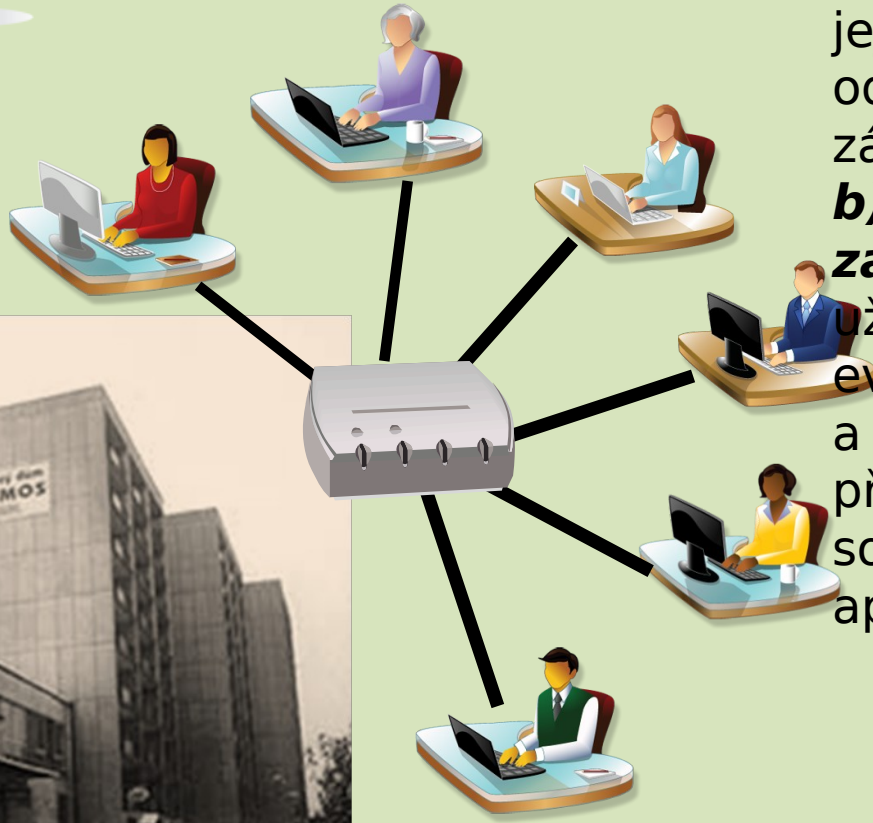
- Správa studentské počítačové sítě
  - vznik sítě
  - administrace sítě
- Základní zabezpečení
  - bezpečnostní hrozby
  - antiviry
  - firewall
  - aktualizace
  - hesla
  - monitoring sítě

INFORMAČNÍ A ADMINISTRAČNÍ SYSTÉM

Pawouk 2010

# Správa studentské počítačové sítě

# Jak to všechno začalo




V souvislosti s provozem bylo nutno zajistit:

***a)Samotnou správu sítě*** - zajištění funkčnosti jednotlivých síťových prvků, jejich monitoring a odstraňování případných závad

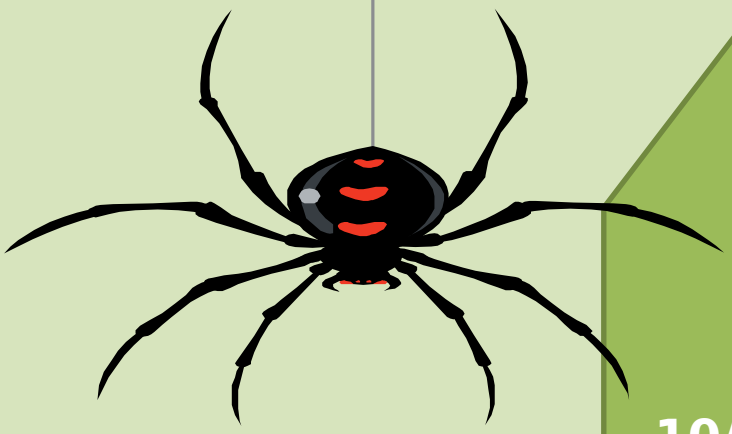
***b)Administrativní záležitosti*** - evidence uživatelů a jejich zařízení, evidence plateb za připojení a další služby, omezování přístupu uživatelů do sítě v souvislosti s těmito úhradami apod.

# Správa sítě a jejich uživatelů


**Cílem** bylo vyvinout vlastními silami informační systém založený na Open source produktech, který bude splňovat následující podmínky:

1)Pro efektivní správu a odstraňování poruch v síti bude umožňovat kdykoliv přístup k aktuálním a detailním informacím o jednotlivých uživatelích sítě, připojených zařízení, ale také údajích
o pohledávkách a platbách za jednotlivé poskytované služby.
2)Vzájemně provázat administrativní činnosti se samotnou správou a maximálně toto spojení zautomatizuje.
3)Bude zajišťovat všechny činnosti spojené s užíváním sítě - od registrace nového uživatele, přes evidenci plateb, až po ukončení připojení - spojit do jednoho rozhraní a maximálně je zjednoduší.

# Od verze 1.x k P@woukovi



Verze 5.x

10/2007


Verze 6.x (P@wouk)

02/2007



Verze 4.x

10/2006


Verze 3.x

10/2005

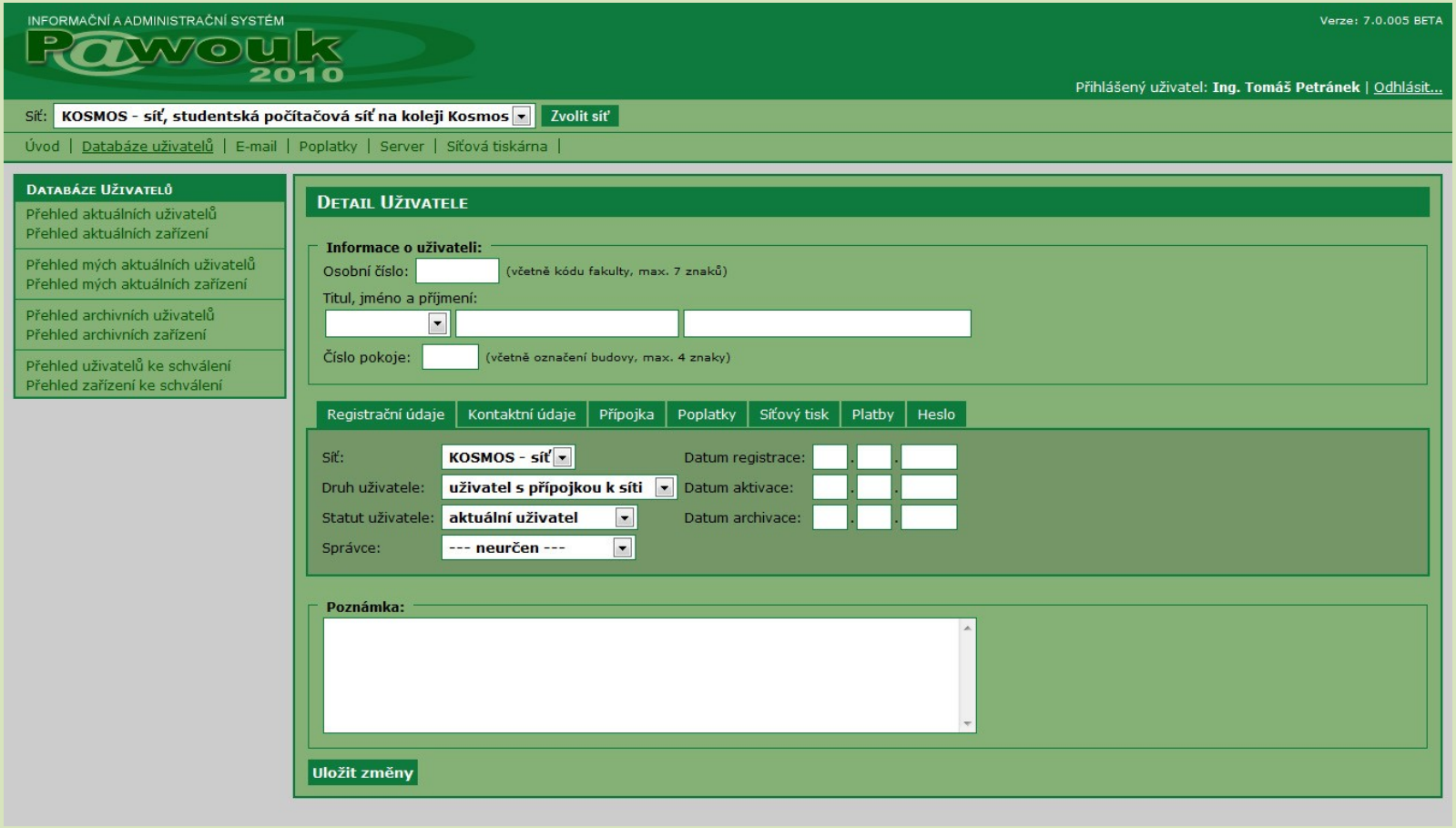
01/2005

Verze 2.x

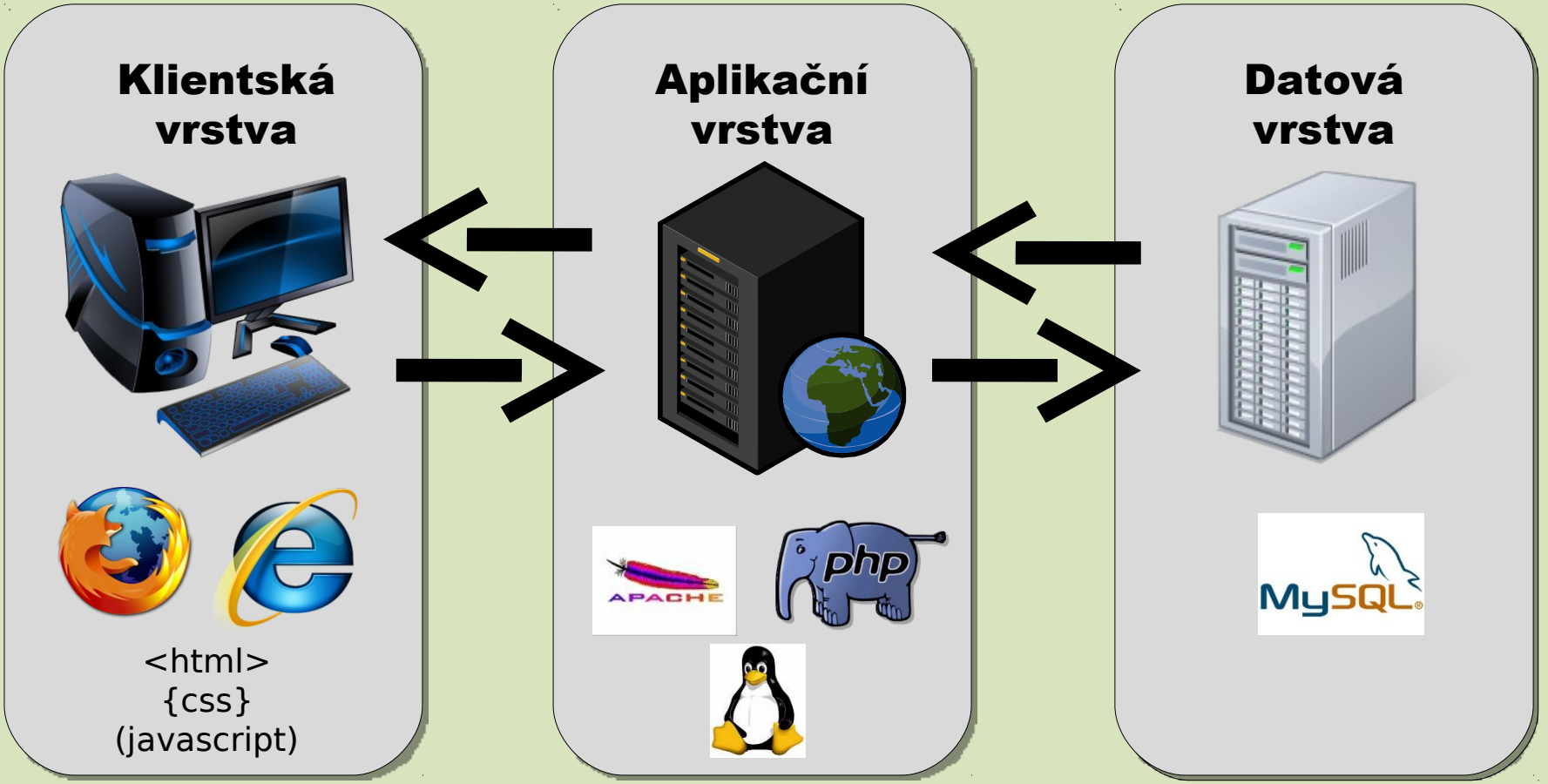

Verze 1.x

09/2004

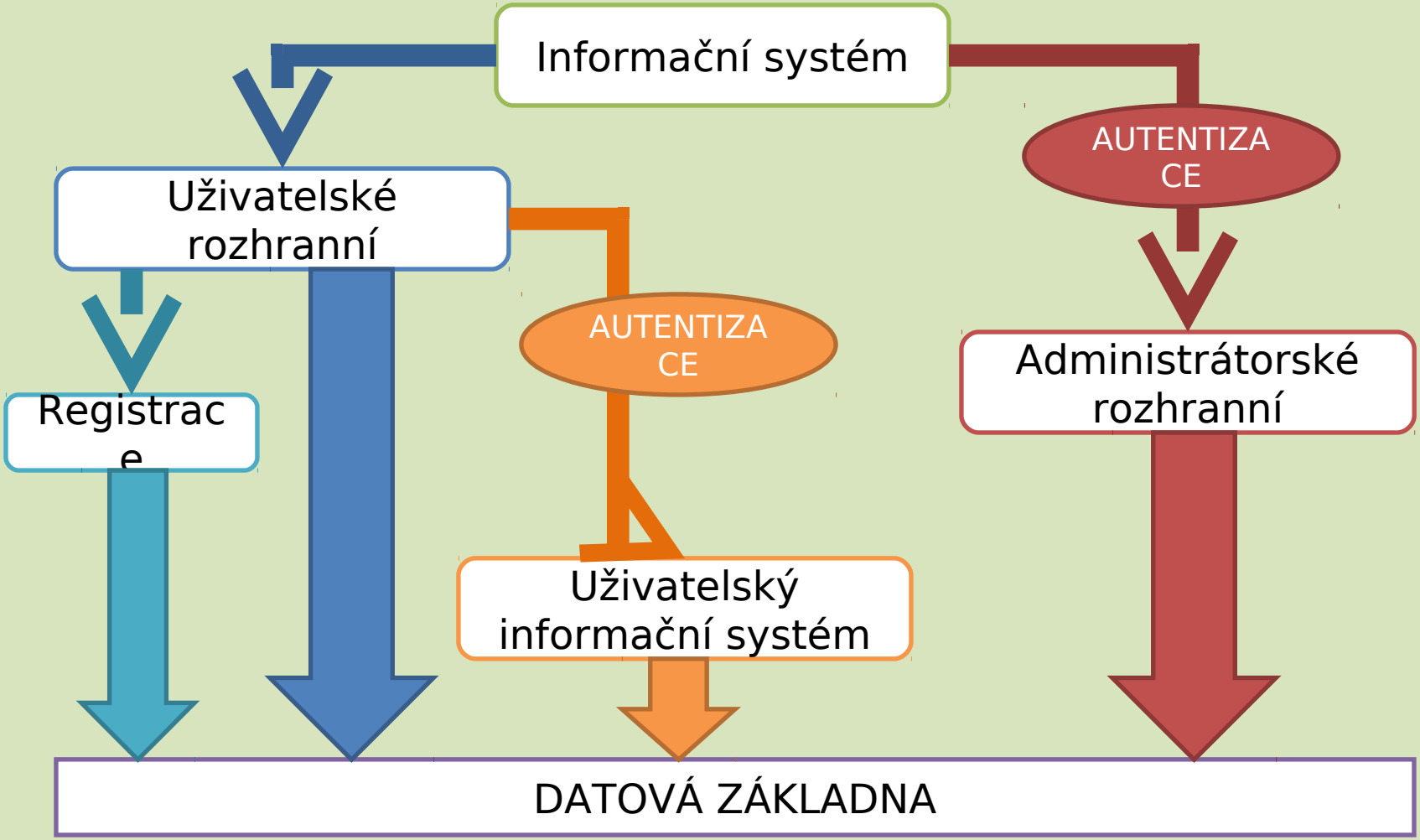
# Verze 7.0
# P@wouk 2010 přichází...



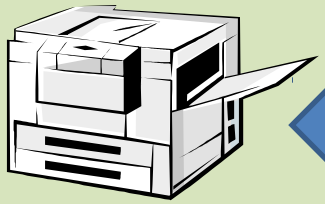
# Architektura systému



# Struktura systému



# Fyzické prostředí a rozhranní systému



DHCP, firewall, Radius

Konfigurační soubory

INFORMAČNÍ SYSTÉM

RESTART

Oprávnění uživatelé vyúčtování tisku

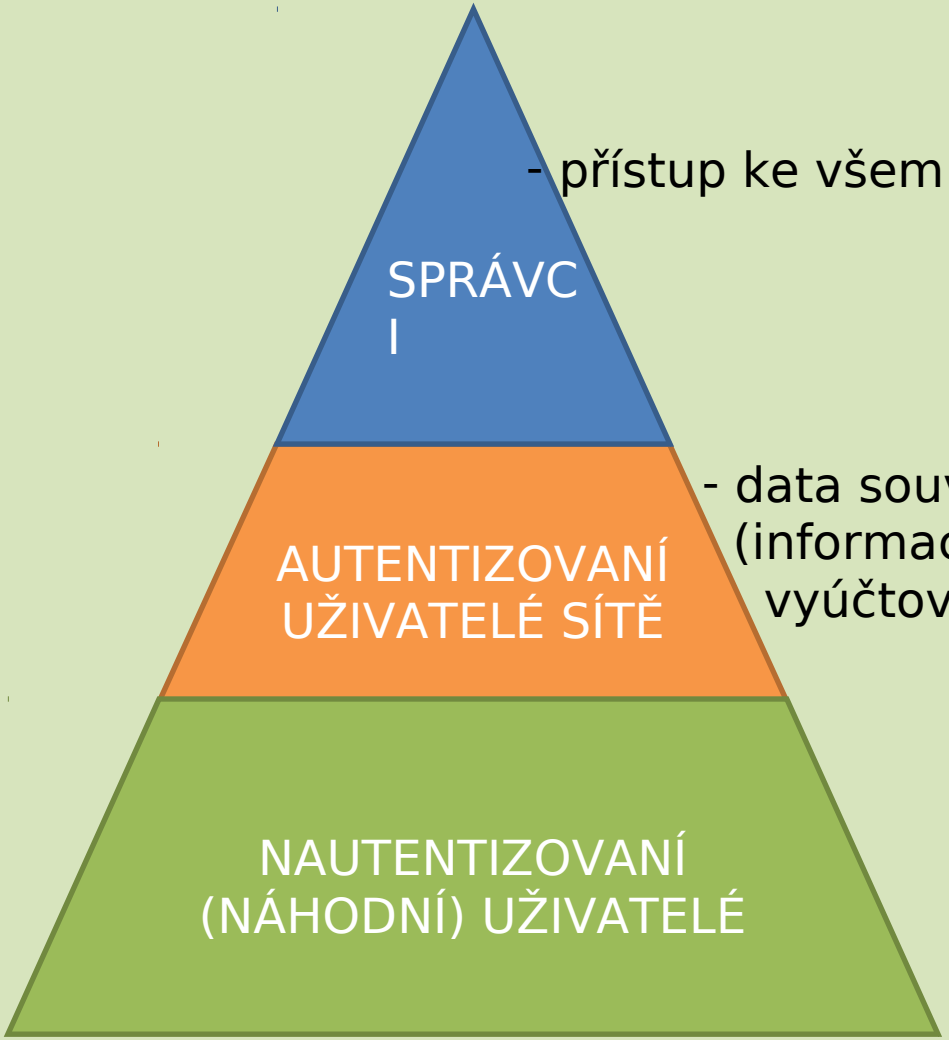
CSV

HTTP DOTAZ/ODPOVĚĎ

- Webová stránka (HTML+CSS)
-Exportovaná sestava (PDF, XLS, CSV)
- Email (automatický, klasický)

**UŽIVATELÉ** (správci sítě + uživatelé sítě)

# Uživatelé systému




- přístup ke všem funkcím (včetně aktivních operací)

- data související s jejich užíváním sítě (informace o uživateli, zařízení, přípojce, vyúčtování apod.)

- obecné informace o síti, návody, možnost registrace

# Funkcionalita

- ***webová prezentace sítě*** – prezentace základních údajů o síti, zveřejnění důležitých dokumentů, návodů a kontaktů,
- ***jednoduchý redakční systém pro správu webové prezentace***,
- ***registrace nových uživatelů služeb sítě prostřednictvím webového formuláře***, možnost schválení/zamítnutí nově registrovaných uživatelů,
- ***evidence uživatelů a připojovaných zařízení*** – databáze s údaji o uživatelích služeb sítě a jejich zařízení včetně archivace těchto údajů, možnost prohledávání, filtrování, zobrazování a export přehledů,
- ***rozhranní pro e-mailovou komunikaci s registrovanými uživateli*** – možnost odeslání jednotlivých i hromadných e-mailů na uživateli registrované e-mailové adresy,
- ***rozhraní pro vnitřní komunikaci mezi správci sítě***,
- ***evidence poplatků*** – zpracování a evidence přijatých plateb za služby sítě od uživatelů, tisk stvrzenek a generování příslušných ekonomických a účetních sestav,
- ***evidence a účtování tisku na síťové tiskárně*** – evidence počtu stran vytištěných jednotlivými uživateli na síťové tiskárně, zpracování vyúčtování za tento tisk a odeslání vyúčtování prostřednictvím e-mailu, export oprávněných uživatelů do tiskového systému, import dat z tiskového systému pro účely vyúčtování,
- ***generování pravidel firewallu, skriptu pro DHCP server a konfiguračního souboru pro Radius server*** na základě stanovených parametrů,
- ***rozhranní pro snadnou administraci samotného informačního systému***,
- ***rozhranní pro uživatele síťových služeb umožňující zobrazení a editaci vybraných údajů*** (přehled registrovaných údajů o uživateli a zařízení, změna hesla, restartování zapomenutého hesla, přehled pohledávek a poplatků apod.).
- ***export vybraných dat***
- ***možnost členění sítě*** *(na sítě a virtuální podsítě)*

# Bezpečnost a zálohování

- *zajištění různé úrovně přístupových práv*
- *monitorování veškerého přístupu k systému a aktivních operací na základě autentizace a jednoznačné identifikace uživatele (autentizace - weauth a dot1x a logování)*
- *možnost zálohování dat i aplikace prostřednictvím standardních nástrojů pro MySQL a GNU Linux,*
- *bezpečnostní opatření administrativní povahy (vhodné zabezpečení hardwarových součástí, ochrana osobních údajů)*

# Více informací o projektu

*http://pawouk.bp.opf.slu.cz/*

# Bezpečnostní hrozby

# Bezpečnostní hrozby

*Cílem útočníka je infikovat/napadnout počítač, umožnit vzdálený*

*přístup jiným osobám, získat citlivá (osobní) data.*

- *Viry*
- *Šíření malware*
- *Útoky na určitý typ slabiny*
- *Síť napadených počítačů (Botnet)*
- *Sociální inženýrství*
- *Phishing*

# Bezpečnost a zálohování

***Sociální inženýrství***

- *Metoda využívána k získávání důležitých informací od uživatelů „bez jejich vědomí”*
- *Zneužívání vlastností lidí*
- *důvěřivost, neznalost, ochota pomoci druhým, obava, nepodezíravost, naivita, hloupost*

***Phishing***

- *podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) od obětí útoku.*
- *Tato technika funguje na principu rozesílání podvodných emailových zpráv, které se tváří jako oficiální žádost např. banky nebo jiné instituce*

# Antiviry

***Antiviry:***

*Avast, AVG, NOD32, Microsoft Security Essentials*

***Nástroje pro odstranění spyware:***

*Ad-Aware, Spybot Search & Destroy, Spyware Terminator, Hijackthis, Combofix*

***Nástroje pro odstranění rootkitů:***

*Microsoft Rootkit Revealer*

***Online antiviry a kontrola souborů***

***Pozor na falešné antiviry!***

*32% počítačů, které jsou chráněny antivirem, jsou napadeny*

*(zdroj: net-security.org).*

# Firewall

*Jde o bezpečnostní software, který kontroluje komunikaci počítače*

*s ostatními počítači v síti.*

***Brána firewall Windows Vista/7***

- *Obousměrná kontrola komunikace.*
- *Při prvním připojení do neznámé sítě se systém zeptá na síťové umístění počítače. K dispozici jsou celkem tři profily Doména, Privátní síť a veřejná síť.*
- *Ve Windows XP SP2 poskytuje brána firewall pouze základní ochranu!*

***Ostatní firewally:***

- *Comodo Firewall, ESET Smart Security, AVG Anti-Virus plus Firewall*

# Aktualizace

***Proč software aktualizovat?***

- *databáze definic (antiviry),*
- *oprava bezpečnostních chyb,*
- *oprava chyb, které mohou způsobit ztrátu dat,*
- *oprava chyb ovlivňující stabilitu či chování,*
- *nové funkce*

***Jak a kdy software aktualizovat***

*služba Windows Update, služba automatické aktualizace*

*Nutná je především aktualizace OS, antiviru, webového prohlížeče*

# Hesla

*Průměrný uživatel používá k přihlášení na webové služby velmi slabá hesla*

- *9% uživatelů má heslo dlouhé jen 4 znaky nebo méně*
- *ovšem heslo o maximální délce 6 znaků (pořád slabé) používá více než 50% lidí!*
- *zjištění čtyřmístného hesla tedy brutal-force útokem zpravidla trval maximálně 40 hodin, v praxi je to ale mnohem méně*
- *odhalení pětimístného hesla by bylo jisté maximálně za 24 dní,*
- *pokud máte maximálně šestimístné heslo, prodloužila by se maximální doba zjištění na téměř 2,5 roku, nicméně platí, že v případě zapojení více počítačů se doba zkrátí*

# Hesla

***Nepoužívat nevhodná hesla!***

*jména, rodná čísla, adresa, názvy, běžné znaky, slovníková hesla*

***Jak tedy zvolit správné heslo?***

*Nejlepší heslo by mělo splňovat všech 5 kritérií:*

- *jednoduše zapamatovatelné*
- *dostatečně dlouhé*
- *složeno z co největší škály znaků, včetně speciálních*
- *nemělo by obsahovat slovníkové výrazy*
- *mělo by být pro danou službu unikátní*

# Bezpečnostní desatero

- *Používejte osobní firewall, antivir, pravidelně aktualizujte.*
- *Používejte dostatečně silná hesla.*
- *Nepoužívejte všude stejná hesla a hesla si měňte.*
- *Neinstalujte neznámé aplikace a doplňky.*
- *Vždy se odhlašujte.*
- *Neklikejte na neznámé odkazy.*
- *Nepoužívejte cracky a keygeny.*

INFORMAČNÍ A ADMINISTRAČNÍ SYSTÉM

Pawouk 2010

# Děkuji za pozornost