**Sdílení technických zařízení sítě**

Síť LAN umožňuje používat všem účastníkům sítě společná technická zařízení. Obvykle se jedná o velkokapacitní disky, laserové tiskárny, a další speciální hardware. Tuto službu si vynutily ekonomické důvody, aby byl zajištěný kompromis mezi vysokou cenou některých zařízení a potřebou jejich používání více účastníky.

Sdílené prostředky jsou typicky ostatním počítačům nějakým způsobem nabízeny, například lze zobrazit všechny dostupné sdílené prostředky v síti. Někdy je však nutné, aby uživatel přesně znal název a umístění sdíleného prostředku. Klienti si sdílený prostředek vhodným způsobem připojí, například jako další disk (Microsoft Windows) nebo jako obsah vybraného adresáře (unixové systémy). Uživatel pak pracuje se sdílenými prostředky podobným způsobem, jako by byly přímo připojené k jeho vlastnímu počítači, takže komunikace přes počítačovou síť je mu skryta (např. pracuje se soubory a adresáři stejně, jako by byly na jeho vlastním pevném disku).



**Sdílení společných dat**

Tento důvod bývá nejčastější příčinou budování počítačových sítí LAN. Všichni uživatelé sítě mohou v síti využívat a zpracovávat společná data. Tato služba se používá, jakmile potřebuje větší počet pracovníků přístup ke stejným datům.

Sdílené prostředky a data jsou typicky chráněny nutností [autentizace](http://cs.wikipedia.org/wiki/Autentizace) uživatele přihlašovacím jménem a heslem (možné jsou i jiné autentizační mechanismy). Po úspěšné autentizaci jsou dále aplikována přístupová oprávnění ([oprávnění v systému souborů](http://cs.wikipedia.org/wiki/Opr%C3%A1vn%C4%9Bn%C3%AD_v_syst%C3%A9mu_soubor%C5%AF), oprávnění tisknout atp.). Konkrétní detaily jsou závislé na použité [platformě](http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_platforma).

V případě [programátorské chyby](http://cs.wikipedia.org/wiki/Program%C3%A1torsk%C3%A1_chyba) může na obou stranách síťové komunikace vniknout [bezpečnostní problém](http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_bezpe%C4%8Dnost), který označujeme jako [zranitelnost](http://cs.wikipedia.org/wiki/Zranitelnost). Program využívající zranitelnost je pak [exploit](http://cs.wikipedia.org/wiki/Exploit), který umožňuje zranitelnost zneužít. Proti nim se lze chránit zejména [principem nejmenšího oprávnění](http://cs.wikipedia.org/w/index.php?title=Princip_nejmen%C5%A1%C3%ADho_opr%C3%A1vn%C4%9Bn%C3%AD&action=edit&redlink=1), pravidelnými [aktualizacemi](http://cs.wikipedia.org/wiki/Aktualizace_%28software%29) softwarového vybavení, použitím [firewallu](http://cs.wikipedia.org/wiki/Firewall), [VPN](http://cs.wikipedia.org/wiki/Virtu%C3%A1ln%C3%AD_priv%C3%A1tn%C3%AD_s%C3%AD%C5%A5) (virtuální privátní sítě) a podobně.

**Monitorování účastníků sítě**

Výhodou služby je hlavně kontrola práce v síti. Monitorování umožňuje zobrazovat na obrazovce počítače, obsahy obrazovek jiných počítačů.

Pokud je použit nějaký komplexní monitorovací systém pro dohled serverů, tak jsou většinou dvě základní možnosti pro přístup k informacím.

***Monitorování s agentem***, kdy se na server instaluje speciální klient. Musí tedy být k dispozici agent pro daný operační systém a musí být možnost jej na sever instalovat.

Druhou možností je ***monitorování bez agenta***, kdy se testují vlastní služby serveru nebo se data získávají pomocí určitých standardních protokolů (jako SNMP, WMI, IPMI).

Seznam technologií, které lze pro monitoring použít:

* dostupnost serveru pomocí ping testu
* dostupnost služby pomocí navázání TCP spojení nebo na aplikační úrovni
* události ze serverů - Syslog
* získávání údajů pomocí klienta
* získávání údajů pomocí monitorovacích protokolů WMI, SNMP, IPMI
* sledování síťových toků - NetFlow
* analýza síťových protokolů - network protocol analyzer
* bezpečnost v síti - IDS/IPS



**Použitá literatura:**

KLIMEŠ, Cyril. *Úvod do počítačových sítí*. 1. vyd. Ostrava: Ostravská univerzita v Ostravě, 2003. ISBN 80-7042-865-1.

Sdílený prostředek. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-12-26]. Dostupné z: <http://cs.wikipedia.org/wiki/Sd%C3%ADlen%C3%BD_prost%C5%99edek>

Začínáme s monitoringem sítě. [online]. 2009 [cit. 2012-12-26]. Dostupné z: http://www.samuraj-cz.com/clanek/zaciname-s-monitoringem-site/