IT ve státní správě

Bezpečnost informačních systémů

Informační systém je tvořen souborem hardwarového a softwarového vybavení, záznamovými médii, daty a personálem, který organizace používá ke správě svých informací. Tyto komponenty mohou být cílem působení mnoha různých vlivů na celkový chod systému:

- *fyzické vlivy* (přírodní katastrofy, požáry, únik vody aj.)
- *lidské vlivy* (nevědomě škodící – nedbalí nebo nezaškolení zaměstnanci; vědomě škodící – agenti cizí rozvědky, hackeři, teroristé, organizovaní nebo jednotliví zločinci, agentury shromažďující občas i nezákonně zprávy za účelem jejich prodeje médiím, nespokojení zaměstnanci)
- *technické vlivy* (výpadky a kolísání el. energie, poruchy zařízení)

Riziko realizace těchto vlivů lze eliminovat nebo minimalizovat použitím vhodných protiopatření. Je nutné, aby tyto ochranné mechanismy byly výkonné, přiměřené, aby působily nepřetržitě a aby uživatelům příliš nepřekážely při rutinní práci.

Základní požadavky na bezpečnost informačních technologií jsou:

1. důvěrnost – ochrana před prozrazením informace
2. integrita – ochrana před neoprávněnou modifikací
3. dostupnost – ochrana před neoprávněným odmítnutím služby nebo nemožností poskytnout informaci.

K zajištění bezpečnosti informačních systémů se využívá kombinace různých bezpečnostních mechanismů a opatření (organizační opatření, fyzická opatření, technická opatření, programová opatření, šifrování, zálohování a antivirová ochrana).

V případě, že se organizace rozhodne používat informační systémy k nakládání s utajovanými skutečnostmi, vyplývá jí ze zákona č. 148 /1998 Sb. povinnost tyto systémy certifikovat Národním bezpečnostním úřadem (za IS podléhající certifikaci NBÚ je nutné považovat i zpracování utajovacích skutečností na samostatném PC). Postup a způsob certifikace informačního systému a požadavky na bezpečnost informačního systému jsou specifikovány ve vyhlášce NBÚ č. 56 / 1999 Sb.

Na základě žádosti o certifikaci informačního systému si NBÚ vyžádá předložení bezpečnostní dokumentace informačního systému. Tu tvoří zejména následující podklady:

a) bezpečnostní politika informačního systému a výsledky analýzy rizik
b) návrh bezpečnosti informačního systému
c) sadu testů bezpečnosti informačního systému, jejich popis a popis výsledků testování
d) bezpečnostní provozní dokumentaci informačního systému
e) popis bezpečnosti vývojového prostředí

Vybrané požadavky na bezpečnost informačního systému :

Fyzická bezpečnost – Informační systém musí být umístěn v zabezpečeném prostoru, ve kterém je zajištěny fyzická ochrana před neoprávněným přístupem, poškozením a ovlivněním. Aktiva informačního systému musí být také chráněna před bezpečnostními vlivy a riziky prostředí a musí být zajištěna nemožnost odezírání utajované informace nepovolanými osobami.

Bezpečnost v prostředí počítačových sítí – Při přenosu utajované informace komunikačním kanálem musí být zajištěna ochrana její důvěrnosti (kryptografickou ochranou) a integrity (spolehlivou detekcí záměrné i náhodné změny utajované informace). Přenosu utajované informace musí předcházet spolehlivá identifikace a autentizace komunikujících stran. Připojení sítě, která je pod kontrolou správy informačního systému, k síti vnější, která není pod kontrolou správy informačního systému, musí být zabezpečeno vhodným bezpečnostním rozhraním tak, aby bylo zamezeno průniku do informačního systému.

Ochrana proti parazitnímu vyzařování – Komponenty informačního systému, které nakládají s utajovanou informací, musí být zabezpečeny proti parazitnímu elektromagnetickému vyzařování, které by mohlo způsobit vyzrazení utajované informace. Úroveň zabezpečení je závislá na stupni utajení utajované informace, se kterou informační systém nakládá.

Bezpečnost nosičů utajovaných informací – Všechny nosiče utajovaných informací musí být řádně označeny a evidovány. Mazání utajovaných informací musí být prováděno takovým způsobem, aby získání zbytkové utajované informace nebylo možné nebo bylo vysoce obtížné i při využití speciálních laboratorních metod a prostředků. Ničení nosiče utajovaných informací musí být provedeno tak, aby nebylo možno žádným způsobem utajovanou informaci z něho opětovně získat.

Personální bezpečnost – Uživatel informačního systému musí být autorizován pro činnost v něm. Provozovatel musí zabezpečit proškolování uživatelů informačního systému v dodržování bezpečnostních opatření a správném užívání informačního systému.
V informačním systému se zavádí role bezpečnostního správce informačního systému odděleně od role správce informačního systému. Role bezpečnostního správce informačního systému obsahuje výkon správy bezpečnosti informačního systému (přidělování přístupových práv, správa autentizačních autorizačních informací, vyhodnocování auditních záznamů, aktualizace bezpečnostních směrnic, vypracování zprávy o bezpečnostním incidentu atd.).

Požadavky na bezpečný provoz informačního systému

- musí být zajištěna antivirová ochrana programového vybavení i utajovaných informací
- v provozovaném informačním systému může být používán pouze hardware a software uvedený v dokumentaci a schválený NBÚ
- musí být prováděno zálohování programového vybavení a utajovaných informací. Záloha programového vybavení a utajovaných informací musí být uložena tak, aby nemohlo dojít k jejímu poškození nebo zničení při ohrožení informačního systému
- servisní činnost musí být prováděna tak, aby nemohlo dojít k neoprávněnému přístupu k utajovaným informacím nebo nerušení integrity hardwarového nebo softwarového vybavení vedoucího k kompromitaci utajovaných informací
- v termínech stanovených v bezpečnostní dokumentaci informačního systému a při vzniku krizové situace musí být neprodleně prováděno vyhodnocení auditních záznamů. Ty musí být archivovány po stanovenou dobu
- řešení základních krizových situací – stanovuje, které situace je třeba ošetřit (oheň – kouř – výbuch, voda – záplavy či prosakování tekutin, výpadek proudu, porucha HW, selhání SW, problémy s konstrukcí budov, přírodní katastrofa, sabotáž – terorismus a další)

základní seznam bezpečnostních incidentů – projev počítačového viru nebo jiného nežádoucího SW, kompromitace hesla nebo podezření na ni, proniknutí nepovolané osoby do místnosti s IS nebo pokusy o ně, hlášení auditu operačního systému (nebo aplikačního SW), neobvyklé chování některého uživatele IS nebo neobvyklý postup uplatněný v IS, neoprávněná změna HW nebo SW, konfigurace IS, neúmyslné nebo úmyslné vyzrazení utajovaných informací neoprávněné osobě, nedodržení předpisu o ukládání výměnného pevného disku nebo přenosného počítače do úschovného objektu aj.

Předpokladem pro vypracování technického řešení je navržení komunikační infrastruktury pro jednotlivá konkrétní řešení státní správy. Přípojným bodem páteřní sítě je komunikační uzel umístěný v prostorách budov státní správy dislokované na daném teritoriu. Přípojné segmenty státní správy jsou standardně řešeny pronajatou digitální linkou zvoleného telekomunikačního operátora.

Základem technického řešení kompaktní sítě státní správy je vybudování zcela oddělené sítě správních agend a vedle ní zcela nezávislé sítě pro ostatní aplikace, s případným využitím již existující síťové infrastruktury. Všem je společné, že sítě správních agend má vyhrazen aktivní prvek (při mimořádných nárocích na počet pracovišť více prvků) typu (L2) přepínač (switch). Na něj jsou připojeny stanice správních agend a jedním optickým portem s využitím konvertoru je připojen ke směrovači (routeru) v datovém stojanu . Z bezpečnostních důvodů má naprosto zásadní význam, aby tento prvek byl plnohodnotným přepínačem a nebyl sdílen s ostatními částmi sítě. Musí rovněž umožňovat dálkovou správu a dohled. Síť pro ostatní aplikace je modelově navržena jako přepínaná síť, která primárně zajišťuje dostatečný výkon pro komunikaci mezi většími skupinami účastnických stanic a servery jednotlivých služeb a aplikací. Předpokládá se podpora linkového protokolu FastEthernet a na vrstvě L2 podpora protokolu IEEE 802.1q (podpora virtuálních sítí). Tím je zajištěna možnost flexibilní optimalizace struktury sítě i u fyzicky nepříznivě rozmístěných pracovišť. Router zajišťuje přístup celé sítě (mimo správní agendy) k Internetu a současně ochranu před případnými útoky zvenčí. U sítí strukturovaných na virtuální podsítě také zprostředkuje komunikaci mezi těmito podsítěmi. Skutečné počty aktivních prvků a jejich detailní podoba (především počty a typy portů) budou muset být stanoveny v prováděcím projektu pro každé pracoviště státní správy. Závisí vedle počtu účastnických stanic, serverů atd. také velmi podstatně na stavebních a geografických dispozicích dané lokality. Jde především o délku kabeláže uvnitř budov, vzdálenosti mezi případnými více budovami a typ použité technologie pro komunikaci mezi vzdálenými budovami.

Aktivní prvky

Sítě správních agend bude v nejjednodušším případě vybavena vlastním switchem s porty 100Mb Fx Fast Ethernetu. Pokud bude nezbytné provozovat správní agendy ve více budovách, bude navržena pro daný případ v rámci prováděcího projektu optimální technologie spojení a bude příslušně upraven počet a typ switchů. Přehled technologií spojení mezi budovami obsahuje další kapitola.

Technologie spojení na větší vzdálenosti

Preferovanou technologií propojení nesouvisejících budov jsou optická vlákna, která zajišťují nejlepší vlastnosti po stránce bezpečnosti přenosu, výkonu a spolehlivosti. Poněkud vyšší pořizovací náklady jsou mnohdy bohatě vyváženy dlouhou morální i fyzickou životností a schopností postupně zvyšovat přenosové rychlosti bez dalších velkých investic a jsou zde také zhodnoceny ekonomické ukazatele pro budování nových optických sítí (odpadají rekonstrukce metalických sítí, zejména výměna metalických kabelů, což představuje nemalou část investičních nákladů).
Méně investičně náročné mohou být bezdrátové technologie. Zejména dobře dostupné jsou spoje podle normy IEEE 802.11b, pracující ve volném pásmu 2,45 GHz. Pro konkrétní projekty je však třeba zvážit jejich reálný výkon a spolehlivost s ohledem na úroveň a předpokládaný vývoj rušení ve volném pásmu v dané lokalitě. Při použití bezdrátových technologií pro správní agendy je naprosto nezbytné vyřešit otázku zabezpečení spoje proti odposlechu, a to pokud možno jinými prostředky, než tato zařízení sama nabízejí – **ty se totiž zatím jeví jako snadno zranitelné**. V úvahu přichází šifrování na aplikační vrstvě, např. mezi terminálovým serverem a emulovaným terminálem nebo vložení speciálních zařízení na síťové vrstvě (např. šifrující routry) mezi části správní agendy a bezdrátová pojítka.
Různé varianty vzdušných pojítek (optická, infračervená) nelze doporučit vzhledem k citlivosti těchto zařízení na počasí, neboť zejména v mlze nejsou schopna poskytnout ani minimální kvalitu spojení.
V částech sítě s omezenými nároky na výkon spoje lze také uvažovat o pronájmu spoje formou služby telekomunikačního operátora, ať už v podobě klasického galvanického dvoudrátového spoje nebo jako digitální služby bod-bod. Zejména u digitální služby je většinou limitující náročnost provozních nákladů při potřebě růstu výkonu spoje.

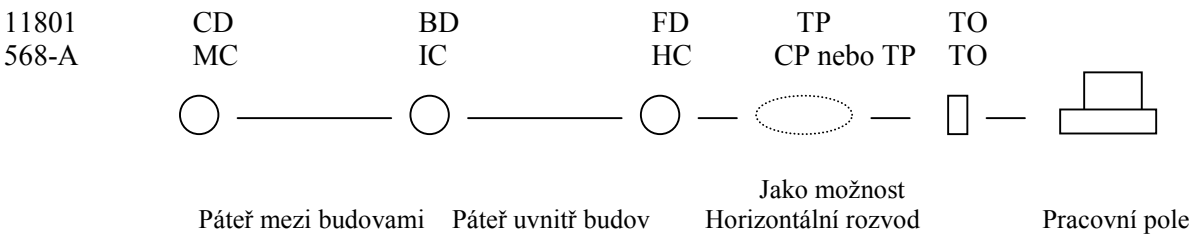
Dále je nutné, aby byly dodrženy všechny normy, které musí splňovat kabelový systém:

ISO/IEC 11801 ……Všeobecné podmínky kabelového systému (mezinárodní)
EN50173 ……..Všeobecné podmínky kabelového systému (evropská)
ČSN EN50173 …….Všeobecné podmínky kabelového systému (česká)

Tyto tři normy (všechny jsou totožné) popisují obecně topologii kabelového systému jako systému skládajícího se ze tří subsystémů: páteřní sítě mezi budovami, páteřní sítě uvnitř budov, horizontální rozvody.

ANSI/TIA/EIA-568-A…… Struktura telekomunikačních rozvodů v budovách (USA)

Tato norma pojednává také o třech subsystémech: páteřní sítě mezi budovami, páteřní sítě uvnitř budov, horizontální rozvody, pouze jiným způsobem značí jednotlivé body sítě.



Kde: CD …. Rozvaděč pro siť mezi budovami
BD …. Rozvaděč pro vnitřní sítě
FD ….. Rozvaděč na patře
TP ….. Transitní bod
MC …. Hlavní přepojovač
IC …. Střední přepojovač
HC …. Horizontální přepojovač
CP …. Konsolidační bod

V těchto normách je možné použít pro páteřní sítě i metalický kabel (např. z MC do HC lze použít kabel UTP na vzdálenost 800m pro kmitočty menší než 5 Mhz). Z důvodu jednotnosti při projektování byly vytvořeny normy pro dovolené vzdálenosti pro jednotlivá přenosová média. Například pro metalický kabelový systém platí norma TIA/EIA TSB-75, která dovoluje v horizontálním vedení spolu s pracovním polem maximální vzdálenost od aktivního prvku 100m. Protože tato norma dále nedostačuje novým požadavkům na zvyšující se vzdálenosti a rychlosti byla vytvořena nová norma pro centralizované optické systémy TIA/EIA TSB-72. Cílem této normy je odstranit rozvaděče FD(HC), protože optika umožňuje přenos na větší vzdálenost než 100m (FastEthernet na 2km) a tím zjednodušit strukturu sítě a snížit její cenu.

Přenosové protokoly

Po takto navržené síti lze provozovat různé typy protokolů (Ethernet, ATM,…). Ovšem každý protokol má s ohledem na rychlost a přenosové médium (metalické vedení, optika) opět své požadavky na vzdálenost mezi rozvaděči.

Pro Ethernet existuje norma IEEE 802.3, která zcela popisuje požadavky kladené na tento protokol. Stejnou technologii popisuje také norma ISO/IEC TR3 8802. V těchto normách jsou definovány maximální vzdálenosti mezi uzly sítě v závislosti na přenosovém médiu. Pro Token Ring platí norma IEEE 802.5 (ISO/IEC 8802-5). Pro FastEthernet (100Base) je platná norma IEEE 802.3u. Pro gigabitový ethernet platí norma IEEE 802.3z, která definuje vzdálenosti pouze pro optický kabel. Pro metalické kabely je v současné době v návrhu norma IEEE 802.3ab, která ještě nebyla schválena.

Kabelové cesty

K tomu, aby byl celý systém správně instalován existuje norma ANSI/TIA/EIA-569-A, která definuje položení kabelů s ohledem na vzdálenosti od silových vedení (rušení), s ohledem na ohyb kabelu (poškození kabelu), množství kabelů ve vodícím žlabu (vliv na rychlost hoření a schopnost samozhášivosti ve žlabu) a další parametry jak nainstalovat správně kabelový systém (optický i metalický).
Propojení mezi budovami definuje norma ANSI/TIA/EIA-758. Tyto normy zaručují kvalitu instalace.

Přenosová média

K tomu. abychom mohli realizovat všechny tyto normy potřebujeme použít nějaké přenosové médium. V současné době jsou k dispozici normy pro následující přenosová média:

Označení	materiál	rychlost	norma
Koaxiální kabel ……	měď …….	-	existuje
Metalika Cat 3 ……	měď, kroucený pár ….	< 16 Mhz	existuje
Metalika Cat 4 …….	měď, kroucený pár ….	< 20 Mhz	existuje
Metalika Cat 5 ……	měď, kroucený pár ….	< 100 Mhz	existuje
Metalika Cat 6 ……	měď, kroucený pár ….	< 250 Mhz	neexistuje
Metalika Cat 7 ……	měď, kroucený pár ….	< 600 Mhz	neexistuje
Metalika Cat 8 ……	měď, kroucený pár ….	< 1200 Mhz/50m	neexistuje
Optika ……..	optické vlákno ……	< 10 Mhz	existuje
Optika ……..	optické vlákno ……	< 100 Mhz	existuje
Optika ……..	optické vlákno ……	< 1000 Mhz	existuje
Optika ……..	optické vlákno ……	< 10000 Mhz	existuje

Pro každé přenosové médium a rychlost existuje zvláštní norma, která upravuje nutné vlastnosti tohoto media, aby byla splněna požadovaná rychlost a podmínky měření. V tomto případě zvolené přenosové médium omezuje přenosovou kapacitu sítě.

Závěr

Nainstalovaná datová síť musí splňovat následující normy a podmínky:

ISO/IEC 11801, TIA/EIA TSB-72 …… hledisko topologie prvků a uzlů.
ANSI/TIA/EIA-569-A ……..… hledisko kvalitní instalace
IEEE 802.3x …… hledisko přenosového protokolu a rychlosti
IEC 61754-19 Edition 1.0.2001-05…… hledisko přípojného bodu konektor VF-45
EIA/TIA 604-7 – FOCIS-7 …….. (Norma pro slučitelnost konektorů pro optické kabely)
Definovaný konektor SG = VF-45. Od ledna 1999 americký patent
MIL – STD – 461D ……Splňuje US Military Standard / norma pro kontrolu elektromagnetického rušení, vyzařování a citlivosti /
Fiber Channel ASC-X3T11……Základ pro Gigabit Ethernet, duplexní konektor, kódovaný, pevně instalovaný protiprašný kryt
Cenelec – norma prEN 50377-3-1…….SG = VF-45
IEC – 60793 – 2
NATO - AMSG

Pokud uživatel instaluje síť, zohledňuje také budoucí rozvoj sítě, který lze specifikovat již v topologii sítě (centrální rozvod, páteřní rozvod, kruh,..) a definicí maximální potřebné přenosové rychlosti. Za těchto podmínek není nutné definovat typ přenosového média, které je již určeno zvolenými normami.

Tyto požadavky plně splňuje optický kabelový systém 3M Volition™ , který je u nás od roku 1999 instalován certifikovanými firmami do nejrůznějších oblastí od průmyslu až po státní správu. Distributorem tohoto systému pro Českou republiku je brněnská firma AVYSYS, s.r.o., která provádí školení pro instalační firmy a s podporou 3M Česko s.r.o. vytváří technickou podporu, pro konkrétní situace.