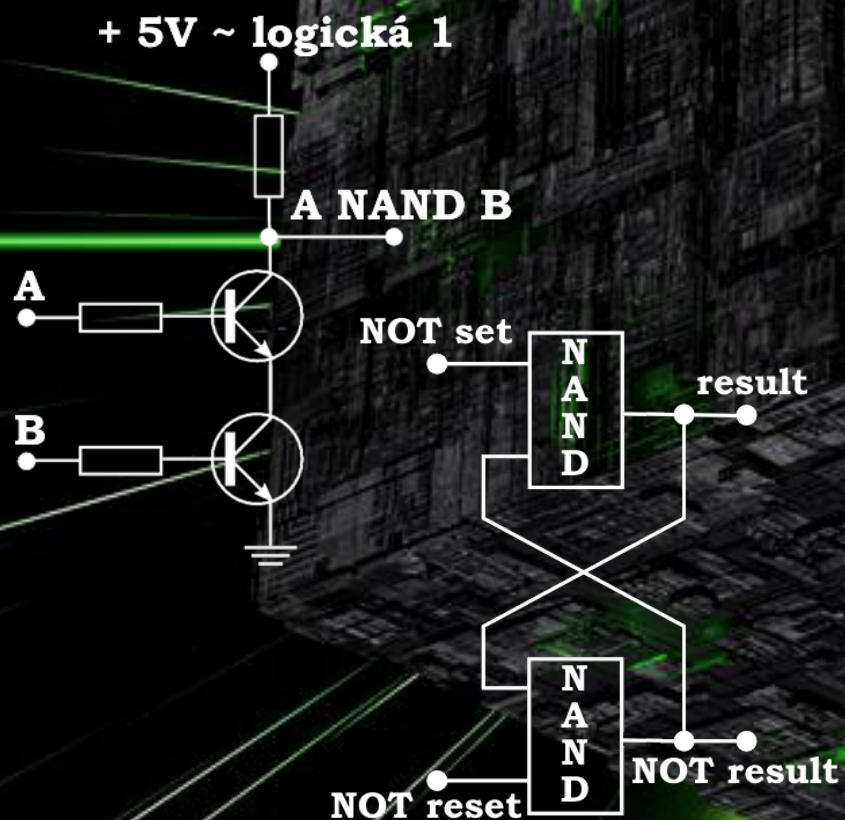


Principy počítačů

Bezpečnost, zálohy, údržba, nákupy



Martin Urza

Cíle

- Tato přednáška má sloužit jako doplnění té minulé.
- Tentokrát nebudeme rozebírat, co dělat, když se nám rozbije počítač, nýbrž jak dosáhnout toho, aby takový stav nenastával příliš často.
- Krom toho se zaměříme na problematiku nakupování nového počítače (či jednotlivých komponent).
 - S důrazem nejen na bezpečnost, trvanlivost, životnost a spolehlivost, ale i na další důležité aspekty, například cenu, protože peníze mohou být utraceny za různé věci; užitečné, ale také zcela zbytečné.
- Dále by přednáška mohla pomoci i tomu, abyste se dokázali rozhodnout, ve kterém případě kupovat nový počítač a kdy raději dokoupit komponenty do starého.

Data

- Obecně jsou data reprezentací informací a nemusí mít vůbec nic společného s počítači.
- Pro účel této přednášky budeme za data považovat informace uložené v počítači, která zároveň nejsou software (tedy nějaké programy), čímž definici dat zjednodušíme.
 - Daty tedy myslíme obsah souborů, se kterými uživatel pracuje pomocí různých programů.
 - Například textové soubory (otvíráme třeba notepadem), obrázky (je možné je otevřít kupříkladu Photoshopem) a tak dále.
 - Software lze vždy sehnat (například na internetu), u dat to nemusí být pravda.

Důležitost dat



• **Cena a důležitost dat je subjektivní!**

- Tatáž data mohou být pro někoho bezcenná a pro jiného doslova nepostradatelná.
- Hodnota každých dat lze nějak (subjektivně) vyjádřit a převést na čas, peníze,
- Některá data lze v případě ztráty získat.
 - Například filmy, seriály, muzika, to vše je možné stáhnout a neshdíle-li nic dál, je to dokonce legální.
- Jiná data jsou ztracena nenávratně.
 - To se týká toho, co jste sami vytvořili a je to tím pádem originální a neopakovatelné.
- Cenu dat (obecně informací) ovlivňuje řada faktorů.

Cena a hodnota dat



- Cena dat, které lze v případě ztráty opět sehnat, odpovídá času, který je třeba na jejich znovuzískání plus případné škodě, kterou jejich absence způsobí.
- Cenu ostatních dat lze spočítat takto (plus je nutné započítat případnou škodu způsobenou absencí dat):
 - Nejvyšší cena, kterou je někdo ochoten zaplatit.
 - Nejnižší cena, za kterou někdo jiný data „vyrobí“.
- I v případě Vašich čistě osobních dat (nikoliv komerčních), která není možné znovu „vyrobit“, lze použít tuto metodu, protože jejich cena bude nejspíš odpovídat ceně, kterou jste za data ochotni zaplatit.
- Ač jsou tyto závěry přirozené, je třeba si je uvědomit.



Paranooidní ochrana dat



- Z nejrůznějších filmů o „drsných hackerech“ se dozvídáme, že „správné“ je zabezpečit data co nejvíce a bez ohledu na cenu onoho zabezpečení.
 - Nejlepší příklad lze najít ve filmu Firewall, neboť to, co tam předvádí kladný hrdina, je čiré diletantství, které svědčí o nepochopení problematiky (správný přístup je ten, který ve filmu zvolili jeho šéfové-záporáci).
- **Vynaložit na ochranu dat více prostředků, než kolik stojí data samotná, je holý nesmysl.**
 - Přesto se s tím lze setkat v reálném světě i mezi takzvanými „odborníky na bezpečnost“.
 - I když častější problém je opačný.



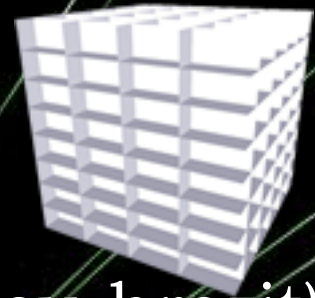
Žádná ochrana dat

- Častějším fenoménem, než jakým bývá přemrštěná ochrana, je (zejména u „běžných uživatelů“) nulová ochrana dat.
 - Když se něco stane, většina uživatelů typicky nejen nemá zálohovaná data, ale ani pořádně neví, která data v počítači má a která z nich chce zachránit.
- Důležitá data (například rozdělaná práce, projekty, seminární práce a podobně) bývají většinou dost malá, takže na jejich zálohu není třeba pořizovat žádné drahé médium, ani ztrácet moc času.
 - Navzdory tomu, že se jedná o pár korun a několik vteřin práce, mnoho uživatelů raději riskuje problémy.

Jak chránit data usilovně, a přesto špatně

- To, že do ochrany dat věnujete hodně zdrojů (času, snahy, úsilí i peněz), ještě neznamená, že jsou data dobře (odpovídajícím způsobem) chráněna.
 - Příkladem z reálného světa je nejmenovaná firma, která si pořídila za nemálo peněz téměř „neprůstřelné“ zabezpečení dat. Po softwarové stránce věci to opravdu skoro nemělo chybu. Vada na kráse se projevila, když někdo odnesl data fyzicky i se serverem za půl milionu a vyšetřování prokázalo, že to mohl být téměř kdokoli.
 - Podobný problém je, když si zálohujete data na externí disk (nebo flashku) a umístíte toto médium do tašky společně s počítačem (ztráta tašky je pak problém).
 - Takových příkladů je k vidění hodně.

Různé roviny ochrany dat



- Je mnoho rizik, která datům hrozí (mohou hrozit):
 - hardwarové poruchy, chyby uživatelů, viry, útoky přes síť (cílené i plošné), fyzická likvidace uložení, krádež, požár, povodeň, libovolná katastrofa, státní/policejní zásahy, ztráta, ale i bizarnější (nešikovské s bagrem, ...)
- Lze podnikat různé kroky k ochraně dat, přičemž většina z těchto kroků je prevencí pouze proti nějakým rizikům (tedy chrání data jen v některé rovině).
- Pro každou rovinu platí, že málo zabezpečená data lze snadno (tedy za nízkou cenou) zabezpečit o trochu víc. Naopak je výrazně dražší (složitější) zabezpečit velmi zabezpečená data o stejnou trochu víc.



Nerovnováha v zabezpečení

- Míra zabezpečení proti rizikům by měla odpovídat pravděpodobnostem rizik a cenám zabezpečení.
 - Data je třeba chránit proti pravděpodobnějším rizikům a takovým rizikům, jejichž prevence je levná.
- Typickou chybou je paranoidní ochrana v jednom směru a téměř nulová obrana ve směru jiném.
 - Často se lze setkat s drahou (a účinnou) softwarovou ochranou a mizernou ochranou fyzickou.
- Útočník není čestný rytíř, proto zaútočí na nejslabší místo, takže síla ochrany odpovídá přesně tomu.
- Nevyvážená ochrana je vždy špatná, neexistuje výjimka (čas a peníze šly vždy využít mnohem lépe).

Příklady chyb při zabezpečování dat

- Pořídit si několik záloh a všechny nosit s sebou.
 - Chrání proti hardwarovému selhání, nikoliv proti krádeži/ztrátě a stálo to dost peněz.
- Koupit si do počítače harddisk na zálohy a ten přišroubovat 1mm od disku hlavního.
 - To vedlo k přehřátí a zničení obou disků.
- Splést si (skoro kdekoliv) tlačítka backup a restore.
- Zálohovat automaticky, často a přepisovat staré zálohy (tady může být horlivost fatální).
- Úžasný firewall, který je tak bezpečný, že uživatele omezuje tolik, až jej dotyčný raději vypíná.
- Některé antiviry jsou horší než mnohé viry.





Bezpečnost není jen o zálohách

- Bezpečnost není jen o ochraně souborů s daty, jedná se o něco komplexního, co se týká celého IS.
- Po informačním systému může být požadováno mnoho vlastností (utajení, dostupnost, integrita, včasnost, současnost, autenticita, anonymita, pseudonymita, ...). Selhat může cokoliv z toho.
- Je-li potřeba víc než holá data, je třeba více ochrany.
 - Chcete-li prezentovat výsledky své práce, ke kterým přistupujete přes síť, je v danou chvíli výpadek sítě a ztráta dat úplně stejný problém.
 - Máte-li dodělat prezentaci v PowerPointu, záloha .ppt souboru nestačí, je třeba nainstalovaný PowerPoint.

Rady pro zálohování



- **Nejde o rady k zabezpečení IS (to by bylo nad rámec přednášky), jde jen o zálohování, což je malá část.**
- Roztřídte svá data na důležitá a postradatelná.
 - Zjistíte, že postradatelná data budou pravděpodobně řádově větší (například filmy, programy a podobně).
- Důležitá data zálohujte na co nejvíce různých médií, která umístěte co nejdál od sebe (fyzicky).
 - Můžete využít média, která přímo nevladníte (ta bývají fyzicky dál), např. různé ftp servery, mail servery,
- Zálohy provádějte v rozumných intervalech tak, aby v případě nahrání zálohy nevznikly moc velké škody.
 - Tyto intervaly závisí na rychlosti práce uživatele.

Údržba



- Ač je ve velkém informačním systému nezbytnou nutností věnovat údržbě mnoho zdrojů, v případě osobních počítačů nic podobného nutné není.
 - To ale neznamená, že údržba není potřeba vůbec.
- Zaprášené a špinavé počítače se přehřívají. Přehřáté počítače přestávají fungovat. Čištění prach odstraní.
- Většina OS potřebuje ke svému běhu nějaké volné místo na disku, to je třeba zajišťovat.
 - Disk lze rozdělit na systémovou a datovou část.
- Objeví-li se nějaká chyba (například se počítač začne vypínat/restartovat), lze očekávat její častější výskyt.
 - Je třeba častěji zálohovat, zkusit to třeba nějak řešit.

Jak vybrat dobrý počítač



- Ač se většina výrobců snaží přesvědčit zákazníky, že potřebují výkonné počítače, už to dávno není pravda.
 - I nejpomalejší počítače, které se dnes vyrábí, výrazně přesahují potřeby uživatelů.
 - 96% veškeré výpočetní kapacity světa vykonává NOOP.
- Když už chcete „lepší počítač“, je rozumnější utratit peníze za více operační paměti.
 - Na takovém počítači lze mít spuštěno více aplikací a přepínat mezi nimi rychleji.
- **Vyšší čísla neznamenají lepší reálný výkon!!**
 - Procesory mají i jiné vlastnosti než taktovací frekvenci.
 - Paměti a disky mají i jiné parametry než kapacitu.

Za co platíme při nákupu PC



- Trh s hardware je relativně svobodný a s minimem státních regulací, což vede k rozumným cenám v tom smyslu, že téměř nic není předražené, ani moc levné. Lze říci, že cena de facto odpovídá kvalitě.
- Platíte tedy vždy za něco „rozumného“ (např. výkon, kvalitu, trvanlivost, záruku, ...).
- Výkon většinou nemá smysl kupovat, trvanlivost i kvalita může souviset se značkou či kategorií zboží (většina komponent se vyrábí i v „serverové verzi“, takové jsou dražší a trvanlivější), záruka je typicky dvouletá, lze ale sehnat i pětiletou.
- Lze také koupit levný počítač s dvouletou zárukou.

Rekapitulace



- Obecně závisí investice do bezpečnosti dat na ceně těch dat (či služeb, pokud jde o informační systém).
 - Nemá smysl dávat příliš mnoho zdrojů do ochrany dat, která nemají moc velkou hodnotu a naopak.
- **Pro běžného uživatele je bezpečnost zejména o zálohování dat, které je třeba nepodceňovat!!**
 - Jako asi všude na světě, u zálohování je třeba myslet, zejména při volbě způsobu a intenzity záloh, ale i u samotného provedení, ale i uskladňování paměťových médií.
- Při nákupu počítače není dobré dát na reklamní slogany o výkonu, nýbrž chtít trvanlivost a záruku.