Kollárova 808/5, Litovel 784 01 obchod@root-it.cz 585 344 056 728 501188 www.root-it.cz

ROOT
IT PROFESSIONAL TEAM

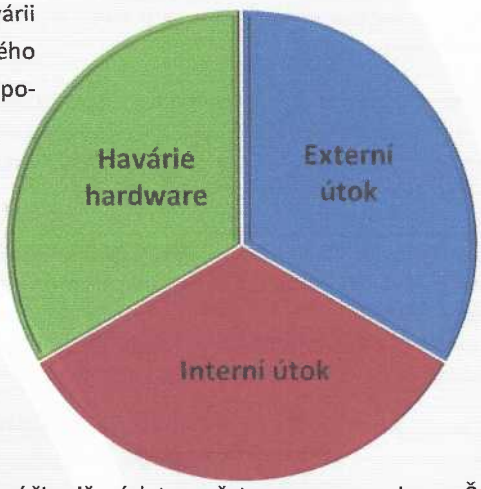
Since 1992

Bezpečnost dat v podmínkách lokálních sítí

Provoz lokálních sítí představuje vynikající způsob jak zvýšit produktivitu, ovšem je nutné mít na mysli také rizika s jejich provozem spojená. Čím větší je množství dat, tím větší jsou také rizika a ztráty, které hrozí. Tato rizika se nedají zcela eliminovat, je možno je pouze do větší či menší míry snížit. Bezpečnost je možno si představit jako zeď, kterou stavíme pro ochranu a tato zeď je jen tak silná, jak je silné její nejslabší místo. Na druhou stranu čím větší zeď postavíme, tím větší je pravděpodobnost, že nás ochrání v případě hrozby.

Bezpečností rizika

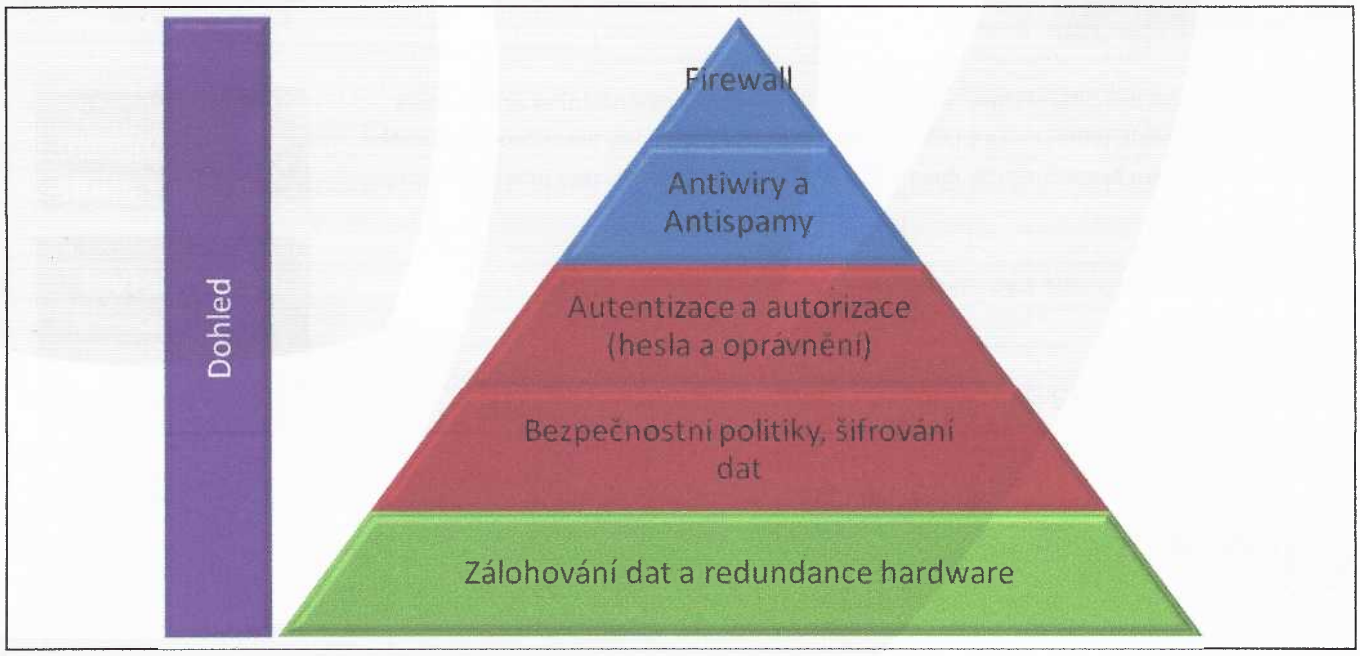
Jedná se především o havárii pevných disků serveru, či celého serveru, nebo klíčových komponent sítě.



Pokus o proniknutí do LAN z Internetu přímo prolomením hesla, nebo pomocí škodlivého kódu infikovaného počítače. K infikaci se využívá e-mailů, stažení kódu z www stránek, spuštěním z CD, DVD, nebo Flash disku. Často se také využívá vyzrazeného hesla uživatelem a podobně.

Pokus o zcizení či zničení dat zaměstnancem organizace. Často zejména u zaměstnanců, kteří dostali výpověď, nebo plánují vlastní podnikání ve stejném oboru jako zaměstnavatel.

Základní způsoby minimalizace rizik



Bezpečnost dat v podmínkách lokálních sítí

Obecně lze říci, že v malých lokálních sítích je téměř nemožné zajistit rozumnou úroveň bezpečnosti bez serveru. Tedy centrálního počítače, který má instalován serverový operační systém, např. Windows Server. Proto všechny další informace budou platit pouze pro LAN (lokální sítě), ve kterých je server instalován.

Ochrana proti havárii, je jednou ze základních ochran, které je naprosto nutné realizovat. Vzhledem ke koncentraci dat na serveru je samozřejmostí řešení redundance (zdvojení) klíčových komponent serveru (pevné disky, zdroje ...) tak aby v případě havárie uživatel nic nepoznal. Zálohování dat je prováděno automaticky bez zásahu lidského faktoru. Pokud dochází k ukládání zálohovaných dat pravidelně mimo areál organizace (do bankovního trezoru nebo do cloudu) je to současně ochrana proti krádeži a živelné pohromě.

Internet dnes představuje mnoho rizik, které je třeba eliminovat. Moderní Firewally dokáží nejen oddělit LAN síť od sítě Internet, ale také umožnit sledování sítě na úrovni protokolů a aplikací a tedy povolit či zakázat provoz specifikovaných programů (např. zakázat provoz Skype, ICQ, či Facebook). Moderní Firewally mají také integrovánu možnost filtrovat provoz Internetu dle hodnocení a například zakázat přístup na stránky s nepovoleným obsahem (porno, militantní stránky či jiné s nezákonným obsahem) .

Instalace antivirů a antispamového řešení je dnes již samozřejmostí. V lokálních sítích je však pro zajištění bezpečnosti důležité používat tato řešení v souladu s bezpečnostními politikami organizace a tedy je nutné použít vyspělé bezpečnostní řešení, které je určeno pro provoz v sítích LAN a umožní zajistit vynucení těchto politik na uživateli. Jinak tato ochrana je-li pouze uživatelská není schopna zajistit bezpečnost a ztrácí smysl.

Pro ověření uživatele a přidělení oprávnění (určení toho ke kterým datům uživatel má či nemá mít přístup) se dnes standardně používá jméno a heslo. Bohužel toto bývá často nejslabším článkem bezpečnosti, jelikož si uživatelé neuvědomují význam hesla. Serverové systémy proto umožňují nastavit politiky silných (složitých) hesel a vynucování jejich pravidelné obměny. Dále je možno také kombinovat používání hesel a USB tokenu, čipové karty či generátoru jednorázových hesel, případně biometrie. Jedná se pak o více faktorovou autentizaci.

Aby bezpečnost byla na přijatelné úrovni, je potřeba nastavit pravidla pro využívání uvedených bezpečnostních prvků v organizaci a kontrolovat jejich dodržování. Je tedy potřeba si definovat bezpečnostní politiky a ty pak pokud možno vynucovat systémově, nebo kontrolovat jejich dodržování. Například je potřeba definovat která data jsou citlivá a ne povinné je pro účely ukládání na přenosná media šifrovat a tím tak předejít jejich zneužití v případě ztráty media.

Pokud ve vaší síti máte data, kterých si ceníte, ale mohla by si je cenit i konkurence a zejména pokud zaměstnáváte více lidí, doporučujeme použít nástroje pro dohled a kontrolu toku informací. Můžete tak přesně zjistit kdo, kdy a jaká data používal, případně kam je kopíroval nebo odesílal. Můžete také díky těmto nástrojům mít přehled o tom jak zaměstnanci využívají svěření IT prostředky (např. PC a internet) a kolik času stráví opravdu prací a kolik času se zabývají jinými činnostmi.

Naše firma používá pro zjištění stavu bezpečnosti takzvaného bezpečnostního auditu, který zjistí stav bezpečnosti, odhalí rizika v LAN a pomůže s definicí metodiky bezpečnosti pro danou organizaci. Metodiku bezpečnosti by měla mít zpracována každá organizace provozující lokální síť.

ROOT Bezpečnostní audit

Bezpečnostní řešení pro malé organizace s méně jak 50-ti uživateli:

ROOT SmallServer
Basic, Standard, Premium

Řešení pro ochranu dat před všemi hrozbami selhání lidského faktoru.

safetica

Pro více informací www.root-it.cz.

ROOT
IT PROFESSIONAL TEAM

Since 1992