Principy a pravidla při nastavení ochrany počítačové sítě před vnitřními uživateli

The Main Principles and Rules of the Computer Network Protection Setting against the Internal Users within the Organization

Ing. Jana Holá, Ph.D., Mgr. Tomáš Hudec
Ústav elektrotechniky a informatiky, Univerzita Pardubice
jana.hola@upce.cz, tomas.hudec@upce.cz

Abstrakt

Vnitřní uživatelé počítačové sítě představují jedno z největších potenciálních nebezpečí z hlediska její bezpečnosti, narušování funkčnosti, snižování efektivity i porušování platné legislativy v této oblasti.

Ve snaze firmy o efektivní využívání počítačové sítě i celé informační a komunikační infrastruktury může významně napomoci nastavení zcela jasných zásad a pravidel, které mají za cíl všechny vnitřní uživatele vhodně informovat, školit a stimulovat k žádoucímu využívání.

Klíčová slova

Ochrana počítačové sítě, zabezpečení počítačové sítě, interní uživatelé.

Abstract

The internal users of the computer network represent one of the main potential dangers from the point of view of its security, disruption of its functionality, limiting its efficiency and also breaking the valid legislative in this field.

In an effort of effective usage of the computer network and the whole information and communication infrastructure of the company the functioning principles and rules within the company can significantly contribute. It is also targeted to inform, train, educate and stimulate the users to covetable usage.

Keywords

Computer Network Protection, Computer Network Security, Internal Users.

Úvod

Informační technologie jsou pro každou firmu strategické investice, bez nichž neobstojí v dnešní tržní konkurenci. V perspektivním podnikání a fungující organizaci se bez informačních a komunikačních technologií nelze obejít. Každá investice by však měla maximalizovat svůj přínos a jednoznačně tak přispět k navýšení konkurenceschopnosti. Je tedy nutné nastavit podmínky ve využívání informačních technologií ve firmě s co největší efektivitou. Důležitým faktorem efektivního využívání informačních technologií je jejich ochrana, zabezpečení neustálé funkčnosti a eliminace všech potenciálních zdrojů jakéhokoliv narušení již v rámci řádné prevence. Každá firma řeší v architektuře celé informační a komunikační infrastruktury preventivní opatření ochrany a bezpečnosti a každý administrátor této infrastruktury ví jak

obrovským nebezpečím pro celé fungování mohou být sami vnitřní uživatelé, přesto mnoho firem se tímto nebezpečím seriózně nezabývá a preventivní práci s vnitřními uživateli zanedbává.

1. Principy a pravidla, bezpečnostní politika

Při vytváření informační a komunikační infrastruktury by měl management firmy dostatečně jasně deklarovat základní cíle, které mají být díky nasazení technologií dosaženy. Dále by měl analyzovat všechny nutné podmínky, které povedou k naplnění určených cílů. Nestačí totiž pouze investovat, je nutné také technologie správně využívat. Z tohoto důvodu jsou interní uživatelé faktorem, který jednoznačně ovlivňuje efektivitu provozu celé infrastruktury. Management musí prosazovat v tomto kontextu jednoznačný zájem na společném cíli s pracovníky – uživateli – využívat technologie jako řídicí a komunikační nástroje, které práci zefektivňují, uživatelům v jejich úsilí napomáhají a uživatelé napomáhají správným využíváním ke správné efektivitě. Aby bylo využívání technologií přínosem, a to zejména správným a bezpečným využíváním uživateli, musí tito uživatelé pracovat v prostředí, které jim nedovoluje infrastruktuře svévolně škodit (např. hardwarové zabezpečení, vymezení práv a personifikované přístupy do systémů a k jednotlivým k aplikacím) a poškozovat infrastrukturu nevědomě díky nedostatku informací či neznalostem nutných pro jejich práci s technologiemi (nastavení interní komunikace a interní školení).

Z uvedených důvodů musí management firmy jasně deklarovat a v rámci celé firmy prosazovat také konkrétní principy a pravidla pro uchování efektivnosti vnitřní sítě, její funkčnost a zejména pak zabezpečení a ochranu.

Souhrn opatření, principů a pravidel vytvoří osu bezpečnostní politiky firmy, kterou je nutné do vnitřního chodu firmy implementovat a dodržovat. S bezpečnostní politikou a jejími konkrétními prvky musí být obeznámeni všichni dotčení pracovníci, kteří pracují s výpočetní technikou jednotlivě nebo k ní mají přístup prostřednictvím sítě (resp. celé informační a komunikační infrastruktury).

Bezpečnostní politika musí zahrnovat všechny fáze ochrany od prevence po řešení incidentů, jejich analýzy a implementace nových bezpečnostních prvků. Bezpečnostní politika v celé šíři tedy zahrnuje:

- pravidla a zásady při výběru dodavatele hardware s důrazem na poskytování záruk a servisu v případě poruch,
- stanovení záložního napájení pro jednotlivé části systému,
- určení dostupnosti konkrétních zařízení po síti,
- role jednotlivých osob a začlenění do skupin podle oprávnění,
- práva jednotlivých skupin k využívání hardware,
- práva skupin k využívání software.

1.1 Využívání hardware vnitřními uživateli

Každý uživatel musí být seznámen s technickými prostředky využívanými v rámci jeho práce, čím lepší je proškolení tím více se preventivně nastaví bezpečné využívání. V rámci administrace pracovník získává určitý stupeň přístupu k hardwaru, který je nastaven podle nároků pracovní činnosti na nastavování hardware (role jednotlivých osob a začlenění do skupin podle oprávnění). Jednotlivých uživatelů, resp. skupinám uživatelů jsou nastavena práva týkající se:

- přístupu k jednotlivým počítačům,
- manipulace s jednotlivými počítači (zasahování do konfigurace a nastavení),
- připojování periférií,
- připojování dalších zařízení k počítačové síti.

1.2 Využívání software vnitřními uživateli

Je velmi důležité nastavit pravidla a jejich dodržování v rámci využívání software. Opět je velmi důležité zařadit pracovníky do skupin podle náročnosti jejich práce na využívání softwaru. Jedná se zejména o přístup, rozsah užívání, instalace a údržbu. Do základního nastavení musí spadat záležitosti zahrnující:

- zásady výběru instalovaného software,
- práva k instalaci,
- instalace aktualizací, patchů,
- zálohování a obnovy,
- správné využívání licenční politiky softwarových produktů,
- personifikované přístupy využívaných aplikací.

Uživatelé musí být proškoleni a motivování k dodržování nastavených pravidel. Je vhodné automaticky provádět pravidelně softwarové audity pro preventivní odhalení potenciálních nebezpečí a případné řešení problémů.

2. Obecné zásady bezpečnosti spouštění síťových služeb

Každý výpadek firemní sítě nebo některé z jejích funkcí způsobuje firmě velké škody, proto je velmi důležité nastavení a bezpečný provoz sítě nepodceňovat a v základním nastavení uživatel – počítač, ale také v úrovni uživatel – firemní síť.

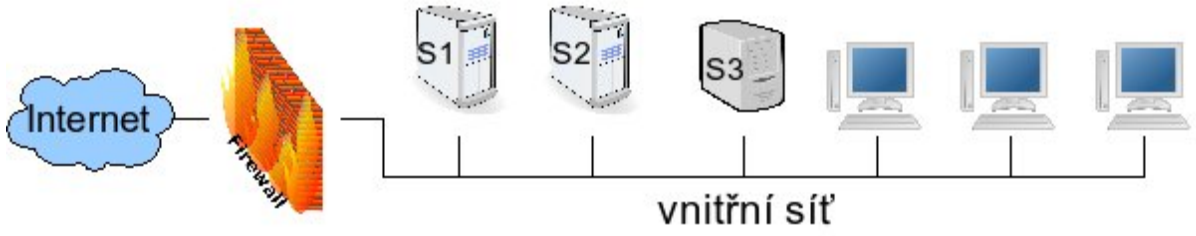
Pro nastavení serverových služeb je nutné ctít pravidlo instalace pouze potřebných a užitečných služeb. Instalací nepotřebných služeb se pouze zvyšuje riziko průniku. Čím větší je počet služeb tím více se zvyšuje pravděpodobnost objevení bezpečností díry. Nejčastější chyby, kterých se administrace firemní sítě dopouští se týkají především:

- chyb v konfiguraci,
- nesprávné manipulace se vstupními daty a/nebo argumenty programů,
- chyb v programech, zejména buffer overflow,
- chyb v jádře systému, neaktualizovaného systému (neinstalované bezpečnostní záplaty),
- spouštění nadbytečných nebo redundantních služeb.

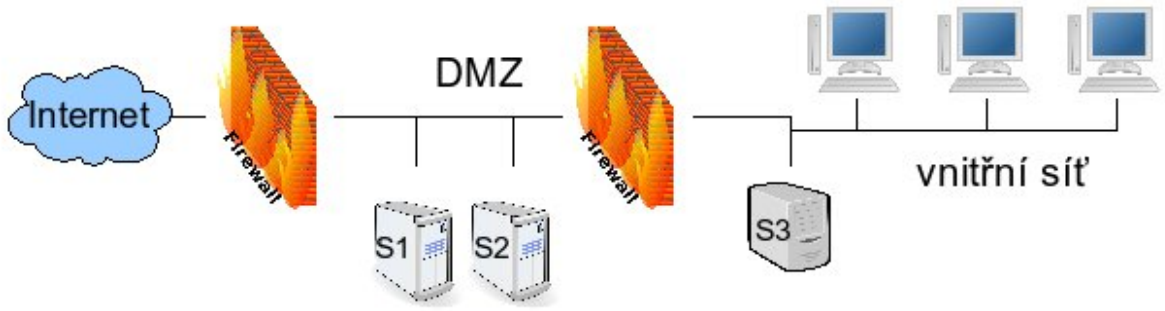
Zkušenosti administrátorů ukazují, že chyby lze očekávat všude, ve všech programech. Nejnáchylnější jsou programy komunikující po síti. E-mailový server, sdílení složek, vzdálené přihlašování jsou nejcitlivější místa pro narušení sítě. Vždy se vyplatí logovat (protokolovat) činnosti všech programů. Logy (záznamy o činnosti) je ovšem třeba kontrolovat a osoby zodpovědné za kontrolu činnosti systémů musí provádět kontrolu logů pravidelně. Tuto činnost lze provádět automaticky, přičemž správce sítě je informován (např. e-mailem nebo pomocí SMS) o případných anomáliích. Nicméně automatická kontrola je nedostatečná, proto je nutné také provádět kontrolu logů ručně. Pro ukládání logů a jejich kontrolu je nezbytný dostatečný kapacitní prostor na discích, aby nedošlo k přeplnění a ztrátě informací.

2.1 Firewall

Dalším prvkem pro zabezpečení ochrany funkčnosti firemní sítě může být firewall. Firewall je místo v síti, které slouží k řízení a zabezpečování provozu. Obvykle je instalován mezi ty části sítě, které mají odlišnou bezpečnostní politiku. Instalace firewallu je vhodná, ovšem neřeší vše. Stále je třeba dodržovat i ostatní zásady bezpečnostní politiky. Zejména je třeba říci, co má být odkud přístupné. Pokud některá část sítě má být více chráněná než jiná, můžeme vytvořit i více firewallů a některé servery dát vně vnitřní (nejzabezpečenější) sítě do takzvané demilitarizované zóny (DMZ). Snižujeme tím rizika, která by vznikla při kompromitování některých serverů, neboť pokud útočník získá kontrolu nad některým (méně důležitým) serverem v DMZ, nezíská tím ještě přístup do vnitřní sítě. V obrázcích 1 a 2 jsou pro vnější přístup určeny servery S1 a S2 a pouze pro vnitřní přístup je určen server S3.



Obrázek 1: Použití firewallu bez DMZ (S1 a S2 jsou servery přístupné ven, S3 je interní server)



Obrázek 2: Použit dvou firewallů a DMZ (oddělení serverů S1 a S2 přístupných vně a vnitřního serveru S3)

Rozdělení celé podnikové sítě do zón napomůže lepšímu zabezpečení systémů. Bezpečnostní politika musí samozřejmě definovat pravidla, která bude firewall uplatňovat. Je potřeba určit i zodpovědné osoby, které určí konfiguraci a nastavení pravidel firewallů, a osoby, které budou zodpovědné za uplatnění takových pravidel. Podceňován bývá také fyzický přístup k firewallům. Bezpečnostní politika musí pamatovat i na určení skupiny osob, které budou mít k firewallům fyzický přístup.

Uživatelé různých oddělení organizace mají obvykle různé požadavky na přístup k síťovým službám, a je proto vhodné umístit firewally i mezi jednotlivé celky vnitřní sítě a rozdělit tím i vnitřní síť na zóny. Firewally mezi těmito zónami je třeba nakonfigurovat s vhodnými pravidly, které budou omezovat přístup vnitřních uživatelů na nezbytně nutné služby sítě. Vytvoříme tím další stupeň zabezpečení sítě a serverů nejen vzhledem k možným útokům zvenčí, ale také před vnitřními uživateli.

2.2 Postupy při narušení bezpečnosti

Často bývá v bezpečnostní politice nedostatečně definován způsob odstraňování následků po narušení bezpečnosti. Pokud je například kompromitován nějaký server v organizaci, je třeba zajistit co nejvíce informací, které pomohou najít útočníka. Zde obvykle pomáhají uložené logy, které by měly obsahovat informace o době připojení jednotlivých uživatelů. Bezpečnostní politika musí v tomto směru zejména obsahovat:

- způsob odpojení kompromitovaných částí sítě,
- způsoby nahrazení nefunkčních nebo odstavených částí sítě,
- osoby zodpovědné za analýzu útoku,
- uplatnění postihů zodpovědných osob při nalezení útočníka a bezpečnostních mezer v systému.

Po odstranění následků je třeba též vyvodit důsledky, které se promítnou do změn v pravidlech bezpečnostní politiky.

3. Závěrem

Ochrana a bezpečnost sítě bývá ve firemní praxi často podceňována zejména v prevenci. Administrace se soustředí na základní prvky zabezpečení a často během empirického procesu s uživateli dochází

k čím dál většímu omezování práv jednotlivých uživatelů nebo skupin. Je to důsledek nedostatečné prevence, která musí být zaměřena nejen na řešení práv uživatelských skupin ve využívání softwaru a hardwaru celé infrastruktury, ale také na interní školení uživatelů a jejich motivaci ke správnému využívání a zamezení zneužívání. Správná disciplína uživatelů je jedním ze stavebních kamenů prevence a velkou úlohu v ní hraje interní komunikace, která musí vycházet z vůle managementu. Management firmy nastavuje pravidla a principy bezpečnostní politiky firmy ve vlastním zájmu, v zájmu zhodnocení investic do informační a komunikační infrastruktury firmy.

Literatura

[1] HOLÁ, Jana. *Interní komunikace ve firmě*. Brno: Computer Press, 2006. 170 s. ISBN 80-251-1250-0.