



Redakční otázky k tématu

BEZPEČNOST PRO SMB

odborného on-line magazínu ICT SECURITY – www.ictsecurity.cz

Nadpis článku:

Bezpečnost vs. omezené finanční i lidské zdroje

Autor odpovědí:

*Jaroslav Mareček, Product Specialist, COMGUARD a.s.,
jaroslav.marecek@comguard.cz*

1) Proč a v čem je SMB jiný sektor, než ostatní? Na co klást větší důraz?

Patrně největší rozdíl je ve zdrojích, a to jak lidských, tak finančních. Jen velmi málo malých a středních firem bude mít dedikovaného administrátora pro bezpečnost (pokud má víc jak jednoho), nemluvě o separátní rozpočtové kapitole. Přes narůstající bezpečnostní hrozby je třeba budovat bezpečnost tak, aby byla co nejsnáze spravovatelná. Velkým bezpečnostním rizikem je totiž frustrace uživatelů i administrátorů kvůli nedostatečné konfiguraci komplikovaných systémů.

2) Kterou oblast bezpečnosti SMB zbytečně podceňuje a na kterou se naopak zbytečně moc soustředí?

V současnosti vnímám jako velmi významnou problematiku ochrany proti úniku důvěrných dat (osobní údaje, databáze o zákaznících, know-how, apod.) Je to výzva pro velké organizace, natož pro ty menší a střední. Přitom hrozba úmyslných krádeží i neúmyslných chyb je trvale přítomna, a to zejména díky vlastním zaměstnancům. U firem do 100 uživatelů doporučuji začít nejprve s šifrováním emailů, celých disků (notebooků) a zejména sdílených dat. Prověřené a přitom cenově výhodné produkty jsou k dispozici od společností PGP či McAfee.

3) Dá se bezpečnost u SMB zvládnout „svépomocí“, nebo je lepší spolehnout na outsourcing?

Záleží to na povaze činnosti organizace, míře provázanosti s dodavateli IT technologií a zároveň konzervatismu zainteresovaných osob ve společnosti. Jen málo firem si dovede představit, že se o jeho data bude starat někdo jiný někde jinde. Proto lze doporučit koncept, kdy organizace vlastní nebo má pronajatu infrastrukturu s bezpečnostními systémy, ale pro jejich správu využívá nějakou formu servisních služeb spřízněné specializované firmy.

4) Je možné vybudovat i v relativně malém prostředí kvalitní bezpečnostní infrastrukturu?

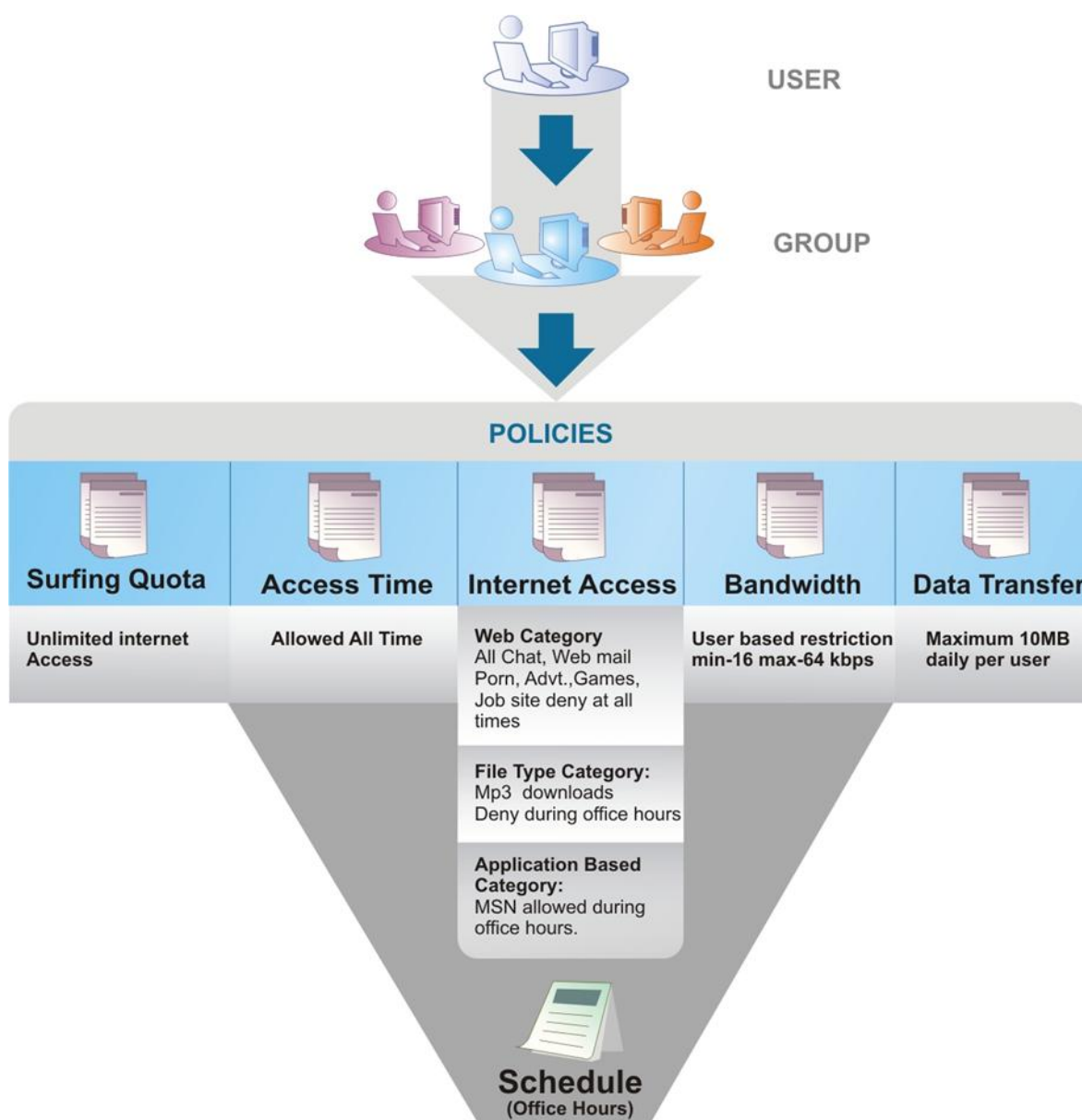
Ano, lze ji sestavit ze tří produktů.

1) Kvalitní konsolidovaná bezpečnostní brána – UTM

Ta by měla sdružovat zejména firewall, IPS pro prevenci narušení provozu (např. VoIP útoky), anti-virus/spyware/spam, URL filtraci pro řízení přístupu k



webu, řízení šířky pásma, VPN pro bezpečný přístup mobilních uživatelů (nejlépe SSL VPN), řízení více připojení do internetu, nástroje pro analýzu provozu v reálném čase a reportovací nástroj na jedné hardwarové platformě se zabezpečeným OS. Pro dosažení maximální efektivity doporučuji koncept řízení provozu na základě identity uživatelů. Takovým řešením je UTM Cyberoam.



Obr. Řízení provozu dle identity uživatelů na základě synchronizace s adresářovou strukturou (MS AD, nebo vlastní přímo na zařízení).

2) Komplexní zabezpečení koncových bodů

Servery, pracovní stanice i mobilní zařízení musí mít kvalitní ochranu proti všem možným, známým i neznámým škodlivým kódům. Standardní antivirus by měl být posílen desktop firewallem a host IPS systémem, zejména u mobilních zařízení (např. notebook). Kritickým bodem z hlediska efektivity této oblasti je centrální správa, díky čemuž již dlouhou dobu dominují celosvětově i u nás produkty společnosti McAfee.



3) Ochrana citlivých dat

Dosud nejméně nasazovaná, možná i podceňovaná vrstva bezpečnosti. Základem je kvalitní šifrování dat, u kterých je to relevantní (viz. otázka č. 2).

5) **Jak v případě SMB co nejlépe a nejefektivněji zajistit organizační stránku bezpečnosti (bezpečnostní politiku)?**

Pokud organizace není „tlačena“ do certifikace ISMS (systém řízení bezpečnosti informací) dle ČSN ISO 27001, lze doporučit kompromis. Čili přečíst si pro inspiraci normy ISO 27001 a 27002, kde se dá snadno získat přehled o tom, co všechno a jak chránit, a následně zdravým selským rozumem eliminovat to, co je příliš nákladné, nebo není v dané organizaci relevantní. Tento přístup může být v budoucnu snadno proměnitelný v rozšíření stávající certifikace ISO 9001 o ISO 27001.