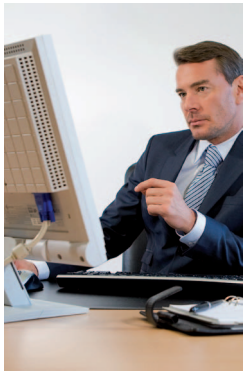
KASPERSKY lab



Malé společnosti: 10 nejdůležitějších odpovědí na otázky zabezpečení infrastruktury IT

Pro malé společnosti je zabezpečení infrastruktury IT stejně důležité jako běžné zakázky. Zatímco svůj podnikatelský záběr dobře znají, zabezpečení počítačů pro ně zůstává záhadou. Zde jsou odpovědi na nejdůležitější otázky ohledně zabezpečení, na které se malé společnosti ptají.

Potřebujeme další software pro zabezpečení?

Většina malých firem používá primárně počítače se systémem Windows. I když společnost Microsoft vylepšila zabezpečení svých operačních systémů s příchodem Windows 7, používání internetu bez ochrany před malwarem je stále nebezpečné. Odpověď na tuto otázku tedy zní "ano". Další ochranný software je nutnost, i pro malé firmy. Měli byste však rovněž zajistit vytvoření odpovídající preventivní strategie pro počítače s jinými systémy, jelikož počítače Macintosh rovněž mívají slabá místa. Nechráněné počítače Macintosh mohou dokonce fungovat jako šiřitelé malwaru a infikovat počítače se systémem Windows – a kdo by chtěl být dodavatelem infikujícím své zákazníky?

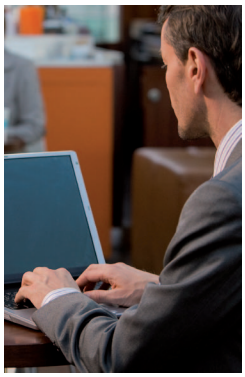
Máme antivirový software. Bude stačit pro zabezpečení infrastruktury IT?

Antivirové aplikace jsou nejznámějším druhem ochranného softwaru. Jsou součástí základního vybavení většiny počítačů doma i v kancelářích. I v malých společnostech by měla být vždy instalována aktuální antivirová ochrana na každém stolním i přenosném počítači. Antivirová aplikace je však pouze jedním prvkem ve vícevrstvé strategii ochrany. Tento druh vícevrstvého systému je doporučen pro společnosti všech velikostí.

Jak vypadá vícevrstvá ochrana infrastruktury IT?

Jelikož jsou malé firmy velmi rozmanité, neexistuje bohužel jednotný seznam zařízení, která lze kdekoliv instalovat. Právní kancelář s pěti cestujícími právníky a třemi sekretářkami má jiné požadavky na ochranu než dvoučlenný malířský tým. Jako určitý kontrolní seznam pro stanovení potřebných součástí ochrany však můžete použít následující body:

- Přístup k internetu: Jak vaše společnost přistupuje k internetu? Používáte jednoduchý směrovač DSL s bránou firewall, nebo vaši zaměstnanci přistupují k internetu pomocí sítě WLAN? Je důležité používat bránu firewall k ochraně vaší firemní sítě. I když by tato brána měla být primárně restriktivní, měla by umožňovat výjimky. Tyto výjimky by však měly být snadno nastavitelné.
- Servery: Má vaše společnost nějaké servery? Pokud ano, tyto vyžadují zvláštní opatření. Servery zpravidla neslouží pouze k uchovávání citlivých dat. Místo toho fungují také jako centralizovaná rozhraní a jsou tak schopny infikovat více



připojených počítačů. Zvláštní ochrana pro servery by měla například reagovat na vysoké vytížení serveru a vyhnout se přílišnému zatížení systému v době špičkového vytížení.

- Stolní a přenosné počítače: Je samozřejmě důležité chránit pracovní stanice vaší společnosti a případné přenosné počítače, které používají terénní pracovníci prodeje. Vedle antivirové ochrany, bran firewall a čerstvých aktualizací by společnosti měly zvážit také šifrování a pravidelné zálohování.
- Zabezpečení webu: Pozměněné webové stránky, spyware na stránkách sociálních sítí a zmanipulované výsledky vyhledávače Google, které uživatele nasměrují na infikované webové stránky, představují hrozby, vůči kterým jsou malé firmy rovněž zranitelné. Proto byste měli nasadit odpovídající ochranná opatření proti hrozbám pocházejícím z internetu a implementovat například filtrování obsahu, které zabraňuje zaměstnancům v přístupu ke škodlivému webovému obsahu.
- Hesla: Malé firmy obvykle používají hesla jako prostředek pro omezení přístupu k informacím. Pro každý systém, ke kterému je třeba přistupovat, by mělo být vytvořeno samostatné, bezpečné heslo. Tato hesla by měla mít délku alespoň 8 znaků a obsahovat směs malých a velkých písmen a rovněž speciálních znaků a číslic. Správce hesel pomáhá uživatelům tato složitá hesla vytvářet, spravovat a používat.

Jak zajistit to nejlepší možné zabezpečení s naším omezeným rozpočtem?

Optimální zabezpečení pro malé firmy poskytují přizpůsobené, komplexní sady jako Kaspersky Small Office Security 2. Takové sady spojují hlavní součásti zabezpečení v jednom balení, což umožňuje jejich hladkou spolupráci. Tyto balíky jsou doplněny "centrem pro správu", centralizovanou konzolí, která umožňuje správcům přehledně sledovat stav zabezpečení sítě a všech počítačů. Tuto centrální konzoli lze použít také k šíření aktualizací a nastavení (včetně např. nastavení přístupu k internetu pro zaměstnance).

Jak si vybrat vhodného poskytovatele softwaru pro zabezpečení infrastruktury IT?

Váš výběr produktu by měl být založen především na požadovaných funkcích. Nejlepšími řešeními jsou kompletní balíky přizpůsobené požadavkům na ochranu malých společností, jako je například sada Kaspersky Small Office Security 2. Pokud požadované funkce nabízí více produktů, měli byste se blíže podívat na možnosti centralizované správy a rovněž na modely flexibilního licencování a nabízenou úroveň podpory. Vaše bezpečnostní opatření infrastruktury IT by měla růst s tím, jak roste vaše firma.

Jak můžeme být informováni o našich licencích?

Důležitým kritériem výběru pro ochranný software je schopnost centralizované správy. Ochranný software by měl umožňovat správu licencí z centrálního bodu. Tato funkce vám umožňuje rychle zjistit, zda nechybějí nějaké licence nebo se neblíží jejich vypršení, a udržuje náklady na správu licencí na minimální úrovni.

Jak flexibilní je zabezpečení infrastruktury IT?

Hotové balíky licencí jsou stejně flexibilní jako vaše společnost, což z nich činí ideální řešení pro malé firmy. Umožňují vám doobjednávání dalších položek – například balíček pěti dodatečných licencí pro klienty a serverové licence – bez velkého úsilí. V dalším licenčním roce lze rovněž objednat menší počet licencí v případě, že se počet počítačů ve vaší společnosti sníží.

Jak lze vytvářet pravidelné zálohy?

Zálohovací modul je pevnou součástí řešení zabezpečení pro malé firmy. Jakékoli kompletní řešení, které zakoupíte, by proto mělo být schopno provádět zálohování. Balíky jako Kaspersky Small Office Security 2 například umí používat rozvrh zálohování k vytváření hodinových záloh a provádět složité číslování verzí důležitých dokumentů.

Je šifrování nezbytné pro naše firemní data?

Šifrování je velmi účinný způsob ochrany citlivých dat ve společnosti. Proto je vhodné použít šifrování vždy, když jde o citlivá data – ať již jde o důvěrné informace o klientech v PR agentuře nebo podrobnosti o bankovních účtech, kterými disponuje finanční poradce. Šifrování dat je naprostou nezbytností na přenosných počítačích, jelikož tato přenosná zařízení mohou být snadno ztracena nebo odcizena na služebních cestách. Když k tomu dojde, cizím osobám zůstanou skryty pouze šifrované informace.

Jak mám přesvědčit své zaměstnance o důležitosti zabezpečení infrastruktury IT?

Zaměstnanci jsou často skeptičtí ohledně nových bezpečnostních opatření, jelikož většina jich omezuje jejich činnost. Na druhou stranu sady pro zabezpečení, jako Kaspersky Small Office Security 2, tento nedostatek kompenzují svou užitečností. Například správce hesel zajišťuje, že se uživatelé mohou rychle a snadno přihlašovat ke všem svým systémům, bez ohledu na použití řady složitých hesel. Poučte své zaměstnance o důležitosti zabezpečení infrastruktury IT a nadneste toto téma na schůzích. Ideálně byste měli jednou či dvakrát ročně uspořádat krátký workshop, který pokrývá obecnou problematiku zabezpečení. Může se zabývat různými tématy, od používání sociálních sítí po bezpečné způsoby používání paměťových zařízení s rozhraním USB. Jakákoli sada pro zabezpečení by vám však měla rovněž umožnit definovat a implementovat zásady upravující používání konkrétních webových stránek nebo nástrojů pro zasílání krátkých zpráv. Pokud do neumí, vaše zásady zabezpečení infrastruktury IT jsou zbytečné.