Nabízíme komplexní řešení IT služeb

Zajistíme komplexní zázemí pro vaši firmu včetně pronájmu, instalace a údržby techniky a softwaru, takže se vyhnete nákladným vstupním investicím i starostem.

K dispozici jsou vám tyto služby:

Office NETWORK
Vybavíme vaši firmu potřebným hardwarem i softwarem, s nulovými pořizovacími náklady a garancí funkčnosti.

Office WIFI
Zajistíme pro vás spolehlivý a stabilní WiFi signál všude, kde jej potřebujete.

Office SECURITY
Učiníme vaši IT infrastrukturu odolnou proti externím i interním bezpečnostním hrozbám.

Office CLOUD
Navrhneme pro vás optimální elektronickou kancelář, kterou podpoříte oběh elektronických dokumentů a bezpečnost při práci s nimi i jejich vyhledávání a archivaci.

Zpomaluje se vám ve firmě internet?

IT bezpečnostní audit vám řekne proč.

- IT bezpečnostní audit probíhal po dobu 1 týdne.
- Nijak nenarušil všední chod firmy.
- Zaměstnanci jej vůbec nezaznamenali.
- Dodali jsme výsledky analýz a doporučení.
- Navrhli jsme optimalizaci provozu sítě.
- Upozornili jsme na rizika v bezpečnosti.
- Nabídli jsme možná řešení.

S NÁMI JE VAŠE KANCELÁŘ BEZ STAROSTÍ!

OFFICE DEPOT s.r.o.
Floriánova 2461, 253 01 Hostivice
IČ: 64942503, DIČ: CZ64942503
tel.: +420 800 771 772
email: infocz@officedepot.com
www.ProcOfficeDepot.cz

IT bezpečnostní audit Office Depot®

Zpomalování internetu ve firmě

Klientem auditu byla výrobní společnost, v níž užívá počítač přibližně 50 uživatelů. Veškeré systémy pak společnost provozuje tzv. in-house na 3 serverech s operačními systémy Windows a Linux. O interní datovou síť se stará externí společnost, se kterou je klient dlouhodobě spokojen. Když se komunikace do/z internetu zpomalila, rozhodl se klient, že využije možnosti prověření sítě specializovanými prostředky a síťovými specialisty.

Uživatelé si delší dobu stěžovali, že v určitých denních dobách dochází ke zpomalení internetové komunikace. Správce následně zjistil, že internetová linka je v některých okamžicích vytěžována na 100 %, což následně vede ke zpomalení jak při načítání webového obsahu, tak k omezení e-mailové komunikace a dostupnosti informačního systému.

Proč k tomu dochází?

Vedení společnosti chtělo ověřit, zda zaměstnanci využívají firemní prostředky skutečně k plnění svých pracovních povinností, anebo spíše ke sledování streamovaného obsahu (youtube.com, stream.cz atd.) a soukromým aktivitám. Klient si chtěl být jist, že vytěžování internetové linky není způsobováno viry nebo jiným škodlivým softwarem, a ověřit, zda se na interní WiFi síť nepřipojují externí zařízení.

Pomůže odborník

Do sítě byla po dobu 1 týdne implementována sonda Fortigate 60C poskytující veškeré pokročilé mechanismy analýzy síťového provozu. Její nasazení trvalo přibližně 30 minut, přičemž výpadek internetové komunikace, tedy dopad na uživatele, byl kratší než 1 minuta. Období jednoho týdne bylo žádoucí pro projevení dopadů všech úloh, které se v síti během pracovního týdne spouští, a hodnocení tak bylo relevantní vzhledem ke všem procesům. Díky získaným informacím a jejich interpretaci zkušeným síťovým analytikem bylo možné nejen zodpovědět klientovy aktuální dotazy, ale i upozornit na některá další rizika.

Co se děje ve firemní síti?

1. V síti nebyly nalezeny signatury škodlivého softwaru (malwaru), klient se tedy ubezpečil, že jím využívaný antivirový software pracuje bez problémů.

2. Aplikační analýza prokázala provoz velkého množství klientů sociálních sítí a sledování videa, a služba filtrování webových stránek toto zjištění potvrzuje. Je tedy zřejmé, že uživatelé svou aktivitu neomezují na pracovní aktivity, ale využívají firemní sítě pro svou zábavu (přístup na portály sociálních sítí a herní portály). Někteří uživatelé během pracovní doby hrají i online hry nebo využívají PtP sítí ke stahování multimediálního obsahu, čímž nejen nadměrně vytěžují síť, ale zároveň vystavují společnost riziku postihů za nelegální sdílení obsahu podléhajícího autorským právům.

Ředitel společnosti se k auditu vyjádřil slovy:

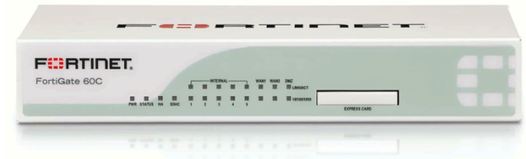
„Chtěli jsme dosáhnout optimálního chodu naší firemní sítě a díky bezpečnostnímu IT auditu od Office Depot se nám to podařilo. Víme, kde jsou naše slabiny, a podle toho volíme následné kroky, které k optimalizaci vedou. Bez auditu bychom nevěděli, kde začít.“

3. Bylo zjištěno, že segment bezdrátové sítě není nijak oddělen a provoz bezdrátové sítě je zajišťován prvky pro domácí použití. Dále bylo nalezeno cca 15 cizích zařízení, která se přes interní síť pravidelně připojují a využívají internetovou konektivitu pro stahování obsahu prostřednictvím webových i PtP sítí.

4. Analýza množství spojení ukazuje nestandardní aktivity některých systémů, které generují nadměrné množství spojení. V souvislosti s objemem přenášených dat bylo rovněž zjištěno, že v síti není instalována služba pro centralizovanou aktualizaci počítačových stanic, které tak stahují aktualizace jednotlivě přímo z internetových serverů – nasazením této služby by bylo možné dosáhnout snížení objemu dat nutných pro aktualizace systému na zlomek velikosti (při počtu 40 PC jde o 40násobné zmenšení přenesené velikosti).

5. Ve společnosti není aktuálně k dispozici kvalitní řízení provozu, aplikační analýza ani odpovídající mechanismy firemního zabezpečení. Nelze tak řídit datový tok dle povahy dat a jejich důležitosti ani analyzovat využití sítě jednotlivými aplikacemi/službami.

Z výše uvedených zjištění (a dle přesných grafů využití sítě v čase) vyplývá, že síť je nadměrně zatěžována jak aktivitou uživatelů (viz body 2 a 3), tak neoptimalizovaným nastavením některých firemních systémů a služeb (bod 5). Navíc tento stav nelze v současné době zcela optimalizovat, protože vzhledem k bodu 5 nemá administrátor možnost jakkoliv prioritizovat či omezovat datový tok.



Doporučení a návrh řešení:

Doporučujeme především nasazení centrální bezpečnostní brány s takovými mechanismy ochrany a řízení, které umožní administrátorovi optimalizovat datový tok na síti, omezit nežádoucí chování uživatelů, zabezpečit vnitřní perimetr a využít aktivního monitoringu, díky kterému lze předcházet zásadním problémům v síti.

Změny k lepšímu

Významným přínosem provedeného IT bezpečnostního auditu bylo pro klienta velké množství získaných dat a jejich vyhodnocení zkušeným specialistou. Díky tomu získal klient jasnou představu o současném stavu, ale i konkrétní návod, jak postupovat při řešení jednotlivých zjištěných nedostatků, a to dle vyjádření míry jejich rizikovosti.

Klientovo hodnocení

- Detailně jsme se seznámili s aktuálními nedostatky v síťovém prostředí.
- Poznali jsme příklady možných zneužití a dopadů, které by mohly společnost v budoucnu ohrozit.
- Za minimální cenu jsme získali zcela konkrétní scénář, jak v řešení postupovat.
- Máme rámcový odhad investic nutných pro realizaci.
- Celý audit proběhl bez jakéhokoliv dopadu na provoz společnosti.
- Nebylo nutné omezovat provoz společnosti ani informovat zaměstnance.