Variace

1

Údržba a ochrana dat

Autor: Mgr. Jaromír JUŘEK

1. Údržba a ochrana dat

Pravidelná údržba počítačů

MOTTO:

"Pravidelná servisní údržba vašeho motorového vozidla sníží riziko technické závady a může předejít závažné nehodě. Stejně tak pravidelná servisní údržba vaší výpočetní techniky sníží riziko havárie vašich počítačů."

Údržba počítačových systémů by měla zahrnovat:

Aktualizace operačních systémů snižuje riziko neoprávněného průniku a následného zhroucení vašich počítačových systémů.

Aktualizace antivirových systémů snižuje riziko nákazy virem. Virová infekce je nejčastějším důvodem ztráty dat.

Aktualizace antispyware zabrání proniknutí škodlivého kódu do vašeho PC. Spyware či Adware může představovat vážné bezpečnostní riziko či snížení komfortu ovládání PC (vyskakující reklamy).

Kontrola zálohovacích mechanismů zajistí, že se vaše data opravdu správně zálohují. Obnovení dat ze zálohy může být poslední naděje na záchranu vašich dat.

Kontrola zabezpečení citlivých dat a pravidelná změna přístupových hesel chrání vaše citlivé informace.

Kontrola funkčnosti firewallů ochrání vaše systémy před neoprávněným průnikem z internetu.

Kontrola přítomnosti nelegálního software, využívaného například vašimi zaměstnanci, může mít zásadní dopad na vaše podnikání. Pravidelná kontrola přítomnosti nelegálního software vám pomůže snížit riziko možného postihu.

Defragmentace disku, kontrola RAID polí, odstranění nepotřebných souborů zrychlí práci vašich pevných disků a pomůže předejít vážným diskovým závadám.

Kontrola funkčnosti a opotřebení hardware (zejména disků a větráčků) zabrání riziku havárie vašeho zařízení.

Audit počítačové infrastruktury

Před zahájením pravidelné údržby vašeho zařízení vám doporučujeme provést úvodní audit stavu vaší výpočetní techniky. Audit vám pomůže zmapovat aktuální stav vašeho IT a odhalit bezpečnostní rizika.

Audit by měl obsahovat tyto části:

- Hardwarový audit
- Softwarový audit
- Bezpečnostní audit

Hardwarový audit

V první fázi dochází ke shromáždění všech informací o dostupném hardware v rámci vaší organizace. Tento sběr se provádí pomocí specializovaného software a jeho výsledkem je přehledný seznam všech zařízení včetně detailního přehledu nainstalovaného hardware i software.

V druhé fázi je vhodné tyto informace odborně posoudit a porovnat se strategickými cíli společnosti. Je možné, že by pro zamýšlený účel vyhovovala jiná struktura zařízení.

Aktuální seznam zařízení je zároveň nutným podkladem pro stanovení metody a frekvence údržby zařízení.

Softwarový audit

Softwarový audit čerpá z podkladů zjištěných v průběhu hardwarového auditu. Zjednodušeně při něm dochází k evidenci používaného software, odhalení nelegálně využívaného software a posouzení vhodnosti aktuální licenční politiky vzhledem k cílům společnosti.

Jedním z vedlejších efektů softwarového auditu může být převod odpovědnosti za legálnost nainstalovaného software na zaměstnance vašeho podniku.

Bezpečnostní audit

Cílem bezpečnostního auditu je především odhalení bezpečnostních rizik provozování vaší výpočetní techniky.

Bezpečnostní audit se zaměřuje zejména na tyto oblasti:

- Pravidelná aktualizace operačních systémů
- Pravidelná aktualizace antivirových a antispywarových systémů
- Spolehlivé zálohovací mechanismy
- Ochrana dat a firemní bezpečnostní politika
- Ochrana proti průniku z internetu
- Fyzické zabezpečení infrastruktury

Odstranění zjištěných bezpečnostních rizik by mělo předcházet veškeré další činnosti.

Audit by vám měl přinést tyto výsledky:

Odhalit bezpečnostní rizika provozu vaší informatiky

Zavést přehlednou, trvalou a stále aktuální evidenci počítačů, software, licencí, instalací a majetku

Přenést odpovědnost za instalovaný software na uživatele počítačů

Šetřit finanční prostředky při nákupu hardwarového vybavení a softwarových licencí

Získat přehled o tom, kdo jaký software skutečně používá a účinně optimalizovat svou licenční politiku

Odhalit provozování nelegálního software a eliminovat rizika vyplývající z porušování autorských práv

Metodika údržby zařízení

Na základě provedení hardwarového auditu máte k dispozici seznam zařízení provozovaných v rámci vaší organizace. Tyto zařízení vám doporučujeme klasifikovat do následujících skupin:

- Server
- PC stanice - kritická (důležité PC, na kterém je například provozováno účetnictví)
- PC stanice - standardní
- Periferní zařízení

Pro každou z těchto skupin nyní stanovte úkony prováděné v rámci pravidelné údržby a jejich frekvenci.

Server - Windows platforma

Perioda 1x měsíčně:

- aktualizace systému a bezpečnostních patchů
- kontrola antivirem a antispywarem
- kontrola logů a chybových hlášení
- kontrola RAID pole
- kontrola skriptů a technik zálohování
- kontrola zařízení ve správci
- kontrola místa na disku
- odstranění nadbytečných souborů

Perioda 1x za 6 měsíců:

- kontrola větráků
- celkový stav serveru
- restart serveru

Perioda 1x ročně:

- mechanická profylaxe
- testy diskového pole
- testy pamětí

PC stanice - kritická

Perioda 1x měsíčně:

- aktualizace operačního systému (Windows XP, Vista, 7, 8)
- zjištění aktuálnosti antivirového programu
- detekce virů a spywaru
- oprava Windows
- odstranění nadbytečných a nepoužívaných souborů
- kontrola zařízení ve správci zařízení
- kontrola disku (checkdisk)

Perioda 1x ročně:

- test pamětí
- kontrola pevných disků, checkdisk s kontrolou povrchu, defragmentace
- mechanická profylaxe
- kontrola větráků
- testy HW (procesor,paměť,...)

PC stanice - standardní

Perioda 1x za 6 měsíců:

- aktualizace operačního systému (Windows 98, XP)
- zjištění aktuálnosti antivirového programu
- detekce virů a spywaru
- oprava Windows
- odstranění nadbytečných a nepoužívaných souborů
- kontrola zařízení ve správci zařízení
- kontrola disku (checkdisk)

Perioda 1x ročně:

- test pamětí
- kontrola pevných disků, checkdisk s kontrolou povrchu, defragmentace
- mechanická profylaxe
- kontrola větráků
- testy HW (procesor,paměť...)

Periferie - tiskárna

Perioda 1x za 6 měsíců:

- test tiskárny zkušební stránkou, nebo interní diagnostikou
- kontrola spotřebního materiálu (toner, válec, vodící dráhy papíru)

Perioda 1x ročně:

- HW profylaxe
- Statistické informace tiskárny

Obsah