



5.20 Nastavení webových/aplikačních serverů

Novelizováno: **2010.12.21.**

Vypracoval	Gestor	Schválil	Platí od	Listů	Příloh
Hlávka	EOS	VS	2010.01.20.	4	

Směrnice platí pro všechny závody Škoda Auto.

Obsah:

- 1 Použité zkratky a pojmy
- 2 Zabezpečení OS serverů
- 3 Zabezpečení aplikačního/webového serveru
- 4 Zabezpečení dalších služeb u serverů přístupných z internetu
- 5 Logování/Auditing

**5.20 Nastavení webových/aplikačních serverů**Novelizováno: **2010.12.21.**

První vydání: 20. 1. 2010

Změna-číslo:

1.

Datum :

21.12.2010

Poznámka :

kompletně přepracováno



5.20 Nastavení webových/aplikačních serverů

Novelizováno: 2010.12.21.

1 Použité zkratky a pojmy

OS	– operační systém
Partition	– logická část pevného disku
Aplikační server	– služba nebo daemon, který zajišťuje běh programů pro zpracování a prezentaci informací.
Webový server	– služba nebo daemon, který vyřizuje požadavky protokolu HTTP(S)
Služba/daemon	– program či proces, který běží na pozadí bez přímého kontaktu s uživatelem

2 Zabezpečení OS serverů

- Na serverech přístupných z internetu smí být používán pouze OS pro který existuje funkční podpora, tzn. jsou vydávány bezpečnostní aktualizace.
- OS všech serveru musí mít nainstalovány poslední stabilní patche pro použitou verzi a musí být zajištěna pravidelná instalace vydaných aktualizací
- Všechny nepotřebné služby/daemoni musí být vypnuté, nainstalované smí být pouze komponenty nezbytně nutné k zamýšlenému účelu serveru.
- Na serveru musí být nainstalován antivirový software s aktuálními virovými definicemi a zajištěnou pravidelnou aktualizací definic, který kontroluje všechny partition serveru.
- OS musí být nainstalován na vlastní partition, ostatní komponenty pak na oddělené partition nebo dalším fyzickém disku.

3 Zabezpečení aplikačního/webového serveru

- Aplikační/webový server smí být používán pouze pokud je zajištěna jeho podpora, tzn. jsou vydávány bezpečnostní aktualizace.
- Na serveru musí být nainstalovány aktuální verze aplikačního/webového serveru včetně patchů a hotfixů a musí být zajištěna pravidelná instalace vydaných aktualizací.
- Aplikační/webový server by měl být spuštěn a provozován pod jiným účtem, než je systémový účet. Administrátor webového/aplikačního serveru by měl k serveru přistupovat pod jiným účtem než je účet pod kterým je aplikační/webový server spuštěn.
- Uživatelský účet, pod kterým je aplikační/webový server spuštěn musí mít omezená práva k systému na nezbytně nutné minimum, nesmí jít o administrátorský účet. Přístupová práva takového účtu k souborovému systému musí být nastavena s maximálním omezením, jen na nezbytně nutné souborové operace a nesmí mít přístup pro změny v systémových souborech. Především se jedná o právo zápisu do binárních a konfiguračních souborů samotného aplikačního/webového serveru. A opačně, přístup k souborům webového obsahu smí mít jen účet webového/aplikačního serveru, s právy omezenými na nezbytně nutné minimum.
- Rozšíření a moduly aplikačního/webového serveru smí být nainstalovány pouze v případě, kdy jsou potřeba pro funkčnost serveru, ve výchozím nastavení jsou všechny zakázány.
- Výchozí nastavení pro komunikaci s aplikačním/webovým serverem je zakázaný přístup pro všechny uživatele, následně se povoluje přístup pro vyjmenované skupiny uživatelů



5.20 Nastavení webových/aplikačních serverů

Novelizováno: 2010.12.21.

4 Zabezpečení dalších služeb u serverů přístupných z internetu

- a) Všechny další služby/daemoni jsou zakázané, pokud nejsou potřeba k provozu serveru.
- b) V případě že jsou služby/daemoni povoleny, musí být používány nejnovější verze a specifikované služby nastaveny v souladu s následujícími pravidly:
 - Služba Telnet musí být nahrazena službou Secure Shell (SSH) nebo odinstalována.
 - Služba FTP musí být (kromě k tomu účelu vyhrazených serverů) odinstalována
 - Poštovní služby - jestliže se nejedná o zařízení vyhrazené pro zpracování e-mailů, smí být služba SMTP přístupná pouze na lokálním rozhraní (IP 127.0.0.1). Poštovní služby musí být zabezpečeny proti hromadnému rozesílání/přeposílání emailů na další adresy (SMTP relay).
 - NFS (Network File System) - služba NFS je možná principiálně pouze při použití důkladnějšího ověření služby RPC (např. AUTH_DES nebo AUTH_KERB)
 - SAMBA - kořenový adresář "/" a adresář "/tmp" nesmí být povolen, povoleny mohou být pouze speciální datové adresáře s přístupovými pravidly, přenos hesla v rámci autentizace musí probíhat šifrovaně

5 Logování/Auditing

- a) Webový/aplikační server musí logovat všechny přístupy a požadavky uživatelů služby. Server musí také logovat všechna lokální i vzdálená přihlášení uživatelských účtů.
- b) Logy musí být ukládány tak aby nemohlo dojít k jejich pozměnění nebo smazání.