5.20 Einstellung der Web-/Applikationsserver

Änderung: 2010-12-21

Ersteller	Fachgarant	Genehmigt	Blätter	Anlagen
Ing. Hauerland	EOS	VS	4	

Die Richtlinie gilt für alle Werke der ŠKODA AUTO.

Inhalt:

E. č. 3276

5.20 Einstellung der Web-/Applikationsserver

Änderung: 2010-12-21

Die neueste aktualisierte Version dieses ITS steht auf der Internetseite „http://cts.skoda-auto.com/“ zur Verfügung. ŠKODA AUTO ist nicht verpflichtet, den Geschäftspartnern die Aktualisierung der ITS mitzuteilen.
Deshalb empfehlen wir nachdrücklich, die ITS regelmäßig auf ihre Aktualität zu prüfen. Diese Dokumente treten am Tag von deren jeweils letzer Aktualisierung in Kraft. Bei abgeschlossenen Verträgen ist die gültige ITS-Version im Moment der Ausstellung der Bestellung ausschlaggebend.
Hinweis: Im Falle von jeglichen Unterschieden zwischen der tschechischen und der deutschen bzw. englischen Fassung dieses ITS ist die tschechische Fassung verbindlich. Die tschechische Fassung steht auf http://cts.skoda-auto.com/ zur Verfügung.

Erstausgabe: 2010-01-20

Änderung Nr.:	Datum :	Anmerkung :
1.	2010-12-21	Vollständig überarbeitet

5.20 Einstellung der Web-/Applikationsserver

Änderung: 2010-12-21

1 Verwendete Abkürzungen und Begriffe

OS – Betriebssystem
Partition – logischer Teil der Festplatte
Applikationsserver – Dienstleistung oder Daemon, die den Lauf der Programme für Verarbeitung und Präsentation der Informationen sicherstellen
Webserver – Dienstleistung oder Daemon, die die Anforderungen des HTTP(S)-Protokolls erledigt
Dienstleistung/Daemon – Programm oder Prozess, der im Hintergrund ohne direkten Kontakt mit dem Nutzer läuft

2 Sicherung der OS-Server

a) Auf den vom Internet zugänglichen Servern darf nur OS eingesetzt werden, für das es einen funktionierenden Support gibt, d.h. für das die Sicherheitsaktualisierungen veröffnetlicht werden.
b) OS aller Server müssen die letzten stabilen Patches für die eingesetzte Version installiert haben und es muss eine regelmäßige Installation der herausgegebenen Aktualisierungen sichergestellt sein
c) Alle unnötigen Dienstleistungen/Daemons müssen ausgestchaltet sein, installiert sein dürfen nur Komponenten, die zum beabsichtigten Zweck des Servers unentbehrlich sind.
d) Auf dem Server muss Antivirussoftware mit aktuellen Virendefinitionen und mit sichergestellter regelmäßiger Aktualisierung der Definitionen installiert sein, die alle Partitionen des Servers kontrolliert.
e) OS muss auf eigene Partition installiert sein, andere Komponenten dann auf separate Partitionen oder auf einer weiteren physischen Festplatte.

3 Sicherung des Applikations-/Webservers

a) Der Applikations-/Webserver darf nur dann verwendet werden, soweit sein Support sichergestellt ist, d.h. dass die Sicherheitsaktualisierungen herausgegeben werden.
b) Auf dem Server müssen aktuelle Versionen des Applikations-/Webservers einschl. Patches und Hotfixes installiert sein und es muss eine regelmäßige Installation der herausgegebenen Aktualisierungen sichergestellt sein.
c) Der Applikations-/Webserver soll unter einem anderen Konto als das Systemkonto gestartet und betrieben werden. Der Administrator des Web-/Applikationsservers sollte auf den Server unter einem anderen Konto als das Konto, unter dem der Applikations-/Webserver gestartet wurde, zugreifen.
d) Das Nutzerkonto, unter dem der Applikations-/Webserver gestartet ist, muss die Rechte zum System auf das unentbehrliche Minimum eingeschränkt haben, es darf sich um kein Adminkonto handeln. Die Zugriffsrechte eines solchen Kontos zum Dateisystem müssen mit maximaler Einschränkung eingestellt sein, nur für unentbehrliche Dateienoperationen und darf keinen Zugriff für die Veränderungen der Systemdateien haben. Es handelt sich vor allem um das Schreibrecht in Binär- und Konfigurationsdateien des Applikations-/Webservers selbst.
Und umgekehrt, den Zugriff zu Dateien des Webinhalts darf nur das Konto des Web-/Applikationsservers mit den auf das unentbehrliche Minimum der eingeschränkten Rechte haben.
e) Die Erweiterungen und Module des Applikations-/Webservers dürfen nur in dem Falle installiert werden, wenn sie zur Funktionsfähigkeit des Servers erforderlich sind, in der Defaulteinstellung sind alle verboten.
f) Die Defaulteinstellung für die Kommunikation mit dem Applikations-/Webserver ist der verbotene Zugriff für alle Nutzer, nachfolgend wird der Zugriff für ausgewählte Nutzergruppen genehmigt.

4 Sicherung der weiteren Dienstleistungen bei den vom Internet zugänglichen Servern

a) Alle weiteren Dienstleistungen/Daemons sind verboten, soweit sie zum Betrieb des Servers nicht erforderlich sind.
b) Im Falle, dass die Dienstleistungen/Daemons genehmigt sind, müssen die neuesten Versionen angewandt und im Einklang mit folgenden Regeln eingestellt werden:
   - Telnet – muss mit SSH ersetzt oder deaktiviert werden
   - FTP – außer eigenen FTP-Server muss deaktiviert werden
   - SMTP – außer eigenen Mail-Server muss SMTP nur für localhost(127.0.0.1) offen werden. SMTP müssen gegen Masse Mailing-und SMTP-Relay gesichert werden.
   - NFS – erlaubt nur mit fortgeschrittener Authentifizierungsmethode (wie AUTH_DES oder AUTH_KERB)
   - SAMBA – Root-Verzeichnis "/" und "/ tmp"-Verzeichnis sind beschränkt; nur spezielle Verzeichnisse für den Datenaustausch mit Zutrittskontrolle sind erlaubt; Kennwort muss immer auf einem verschlüsseltem Weg übertragen werden.

5 Loggen/Auditing

a) Der Web-/Applikationsserver muss alle Zugriffe und Anforderungen der Dienstleistungsnutzer loggen. Der Server muss auch alle lokalen sowie Remote-Anmeldungen der Nutzerkonten loggen.
b) Die Loggs müssen so gespeichert werden, dass es zu ihrer Veränderung oder Löschung nicht kommen kann.