Abschlussprüfung Sommer 2006
Lösungshinweise

Fachinformatiker/Fachinformatikerin
Systemintegration
1197

1 Ganzheitliche Aufgabe I
Fachqualifikationen

Allgemeine Korrekturhinweise

Die Lösungs- und Bewertungshinweise zu den einzelnen Handlungsschritten sind als Korrekturhilfen zu verstehen und erheben nicht in jedem Fall Anspruch auf Vollständigkeit und Ausschließlichkeit. Neben hier beispielhaft angeführten Lösungsmöglichkeiten sind auch andere sach- und fachgerechte Lösungsalternativen bzw. Darstellungsformen mit der vorgesehenen Punktzahl zu bewerten. Der Bewertungsspielraum des Korrektors (z. B. hinsichtlich der Berücksichtigung regionaler oder branchenspezifischer Gegebenheiten) bleibt unberührt.

Zu beachten ist die unterschiedliche Dimension der Aufgabenstellung (nennen – erklären – beschreiben – erläutern usw.). Wird eine bestimmte Anzahl verlangt (z. B. „Nennen Sie fünf Merkmale ..."), so ist bei Aufzählung von fünf richtigen Merkmalen die volle vorgesehene Punktzahl zu geben, auch wenn im Lösungshinweis mehr als fünf Merkmale genannt sind. Bei Angabe von Teilpunkten in den Lösungshinweisen sind diese auch für richtig erbrachte Teilleistungen zu geben.

In den Fällen, in denen vom Prüfungsteilnehmer

- keiner der sechs Handlungsschritte ausdrücklich als „nicht bearbeitet" gekennzeichnet wurde,
- der 6. Handlungsschritt bearbeitet wurde,
- einer der Handlungsschritte 1 bis 5 deutlich erkennbar nicht bearbeitet wurde,

ist der tatsächlich nicht bearbeitete Handlungsschritt von der Bewertung auszuschließen.

Ein weiterer Punktabzug für den bearbeiteten 6. Handlungsschritt soll in diesen Fällen allein wegen des Verstoßes gegen die Formvorschrift nicht erfolgen!

1. Handlungsschritt (20 Punkte)

a) 1 Punkt

VPN Gateway

ba) 2 Punkte

Prüft ankommende Datenpakete mit Pattern Recognition Technologie und anomaliebasierter Analyse auf verschiedene Einbruchsmethoden und verdächtige Daten.

bb) 2 Punkte

Scannt ankommende Netzwerkpakete und erkennt mit Hilfe von Pattern Recognition Technology und anomaliebasierter Analyse Einbruchsmethoden und verdächtige Daten.

bc) 2 Punkte

- Überprüfung des Absenders
- Vergleich mit Realtime Blackhole Lists (RBLs) und Spam-Datenbanken
- Analyse des Headers
- Heuristische Analyse des Inhalts auf Spam-typische Begriffe
- Whitelists und Blacklists

bd) 2 Punkte

überwacht und kontrolliert den Zugriff auf Webseiten
Prüfung der Webseiten auf Schlüsselwörter, Bildinhalte und Textzusammenhänge (z. B. Pornographiefilter)

c) 4 Punkte

Authentifizierung, Autorisierung und Accounting (optional) von Einwahlverbindungen; im Fall der Doll AG Verwaltung der VPN-Clients

d) 3 Punkte

- Anschluss am DMZ-Anschluss der Network Security Appliance
- DMZ ist ein semigeschütztes Netzwerk, das gegenüber dem öffentlichen Internet durch eine äußere Firewall und gegenüber dem internen Netzwerk durch eine innere Firewall abgegrenzt ist.
- Bei einer Kompromittierung des WWW-Servers bleibt das interne Netz geschützt.

e) 4 Punkte

Network Security Appliance ist geeignet, weil

- Anzahl der Benutzer unbegrenzt ist.
- Anzahl der VPN Tunnel unbegrenzt ist.
- Firewall-Datendurchsatz mit 3 000 Mbit/s hohe Belastungen ermöglicht.
- VPN-Datendurchsatz mit 400 Mbit/s hohe Belastungen ermöglicht.
- 1000Base-TX Ports leistungsfähige Anschlüsse vorhanden sind.
- Option für SFP GBIC Ports - leistungsfähige Anschlüsse vorhanden sind.

2. Handlungsschritt (20 Punkte)

a) 4 Punkte

- VoIP (Voice over IP): Telefonieren über ein Computernetzwerk auf der Grundlage des Internetprotokolls
- Die analogen Signale werden digitalisiert und komprimiert.

b) 4 Punkte

- Minimales, verbindungsloses Netzwerkprotokoll
- Kurze Latenzzeit (fehlerhafte Sprachpakete werden nicht wiederholt gesendet) ist Voraussetzung für ein flüssiges Gespräc
- Fehlerfreie Übertragung aller Sprachpakete aufgrund von Redundanzen nicht erforderlich

ca) 2 Punkte

- IP-Adressen der Teilnehmer müssen bekannt sein.
- SIP-Server (SIP: Session Initation Protocol) oder H.323 Gatekeeper

cb) 2 Punkte

- VoIP-Gateway, der die interne VoIP-Struktur mit dem öffentlichen Telefonnetz verbindet.

da) 2 Punkte

Bevorzugte Weiterleitung von Sprachpaketen durch Router (QoS - Quality of Service) oder Switches (Layer 2-Priorisierung)

db) 2 Punkte

- Zeit zwischen der Entstehung eines Signals beim Sender und dessen Wiedergabe beim Empfänger
- Schlechte Sprachqualität bei Latenzzeiten von mehr als 100 mSek

dc) 2 Punkte

- Die Sprachpakete haben unterschiedliche Laufzeiten und gehen daher beim Empfänger mit unterschiedlichen Zeitabständ
- Die verzögerungsfreie Ausgabe der Sprachpakete wird durch einen Pufferspeicher möglich.
- Eine verzögerte Ausgabe von Sprachpaketen führt zu Artefakten.

dd) 2 Punkte

- Sprachpakete erreichen Empfänger nicht.
- Schlechte Sprachqualität durch Verlust mehrerer Sprachpakete

3. Handlungsschritt (20 Punkte)

a) 2 Punkte

Server schickt an Client die im Dienst vereinbarte Information.

b) 6 Punkte

- Arbeitet nahezu überall
- Verbindung zu vielen Netzwerken
- Kompatibilität zu den wichtigen Mail-Plattformen
- Zugriff auf Unternehmensdatenbanken
- Push-Technik
- Optimierung und Komprimierung des Datenverkehrs
- Strenge Sicherheitsstandards

c) 4 Punkte

- Es werden immer alle E-Mails vom Server zum Client übertragen.
- Es wird immer die gesamte E-Mail (mit allen Anhängen) zum Client übertragen. (E-Mail kann erst geöffnet werden, wenn Übertragung beendet ist.)
- E-Mail wird nach Übertragung auf Server gelöscht.

da) 2 Punkte

- Kanalbündelung und damit Erhöhung der Übertragungskapazität
- (praktische Übertragungskapazität bei GPRS und HSCSD bis zu 57,6 kBit/s)
- (theoretische Übertragungskapazität bei GPRS 171,2 kBit/s, bei HSCSD 115,2 kBit/s)

db) 4 Punkte

- Der Funkraum wird nur genutzt, wenn Daten gesendet werden.
- Vom Provider wird vorwiegend die übertragene Datenmenge und nicht die Verbindungsdauer abgerechnet.

dc) 2 Punkte, 2 x 1 Punkt

GPRS
2 500 kByte x 0,001 €/kByte = 2,50 €

HSCSD
2 500 kByte · 8 bit/Byte / 56 kbit/Sek = 357 Sek = 5,9 Min (ca. 6 Min)
0,10 €/Min · 6 Min = 0,60 €

4. Handlungsschritt (20 Punkte)

a) 2 Punkte

Samba Server

b) 2 Punkte

- smb
- Server Message Block

c) 4 Punkte

- Über ssh, Secure Shell (auch Open SSH), textbasiertes Konsolenfenster
- Über X-Emulation, Ausgabe von Linux-Programmen auf die XP-Arbeitsstation
- Fernsteuerung über VNC oder andere Produkte

da) 2 Punkte

Die Daten gehen unverschlüsselt über das Netzwerk und können leicht abgehört werden.

db) 2 Punkte

ssh

dc) 2 Punkte

Putty.exe, WRQ Reflection, Hummingbird Exceed ... (andere, überprüfbare Lösungen sind möglich)

e) 6 Punkte

Windows

Aufgabe	**Befehl**
Befehlsfenster starten	Start/Ausführen/cmd
Zur D-Partition wechseln	d:
Ins Wurzelverzeichnis wechseln	cd \
Ins vorhandene Verzeichnis *Vertrieb* wechseln	cd Vertrieb
Verzeichnis *Exchange* erstellen	md exchange
Inhalt des vorhandenen Verzeichnisses *temp* löschen	del temp*.*
Datei *d:\Programme\aglp.ini* in das Verzeichnis *Temp* kopieren	copy d:\Programme\aglp.ini temp
Kopierte Datei *aglp.ini* in *aglp.in$* umbenennen	rename temp\aglp.ini aglp.in$

oder

Linux

Aufgabe	**Befehl**
Befehlsfenster starten	Linux ist bereits im Textmodus
Ins Wurzelverzeichnis wechseln	*cd /*
Ins vorhandene Verzeichnis *Vertrieb* wechseln	*cd Vertrieb*
Verzeichnis *Exchange* erstellen	*mkdir exchange*
Inhalt des vorhandenen Verzeichnisses *temp* löschen	*rm temp/**
Datei */etc/aglp.ini* ins Verzeichnis *temp* kopieren	*cp /etc/aglp.ini temp*
Kopierte Datei *aglp.ini* in *aglp.in$* umbenennen	*mv ./temp/aglp.ini ./temp/aglp.in$*

5. Handlungsschritt (20 Punkte)

a) 3 Punkte

Nach jedem Wechsel der IP-Adresse muss der DNS-Name in die neue IP-Adresse aufgelöst werden.

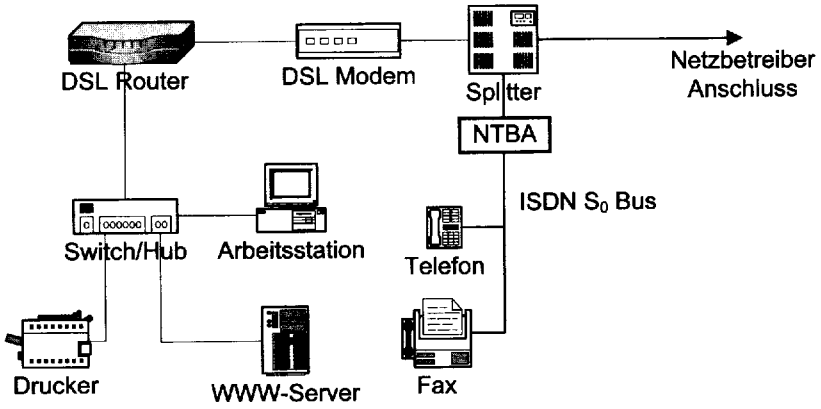
b) 3 Punkte

Bestimmte Provider (z. B. dyndns.com) bieten an, dass deren DNS-Server die IP-Adresse des Klienten (WWW-Server von Frau Ba Änderung der IP-Adresse sofort aktualisieren.

c) 4 Punkte

Update Client ist auf dem PC oder WWW-Server des Heimarbeitsplatzes installiert. Er ermittelt und sendet jede neue IP-Adresse Server des Providers, der die DNS-Adresse in die neue IP-Adresse auflöst.

d) 7 Punkte



e) 3 Punkte

- Upstream des DSL-Anschlusses
- Beim Abruf von Webseiten oder bei Downloads müssen viele Daten schnell zum Client gesendet werden.

6. Handlungsschritt (20 Punkte)

a) 6 Punkte, 3 x 2 Punkte

Netzwerkadresse: 10.46.27.0
Subnetzmaske: 255.255.255.0
Metrik: 3

b) 4 Punkte

Multicast
Router-Bekanntgaben erfolgen nicht als Broadcast sondern über die Multicastadresse 224.0.0.9 nur an die Anwendung RIP-

Vorteil: Geringere Netzlast bei Multicast-Filterung (nur Segmente mit RIP-2-Routern erhalten Router-Bekanntgaben)

Authentifizierung
Authentifizierung von Routern kann erzwungen werden.

Vorteil: Nur von authentifizierten Routern werden Router-Bekanntgaben akzeptiert.

c) 4 Punkte, 2 x 2 Punkte

- Mehrere Clients mit privaten IP-Adressen können gleichzeitig über eine öffentliche IP-Adresse mit dem Internet verbunde (Anzahl registrierter öffentlicher IP-Adressen ist beschränkt. In privaten Netzen werden daher nicht registrierbare private verwendet. Private IP-Adressen können nicht in das Internet geroutet werden.)
- Die privaten IP-Adresssen bleiben dem öffentlichen Internet verborgen (Schutz vor Missbrauch).

d) 6 Punkte

Hinweis: Die Quellports/Zielports 2500 bzw. 2501 sind zwischen 1024 und 65535 frei wählbar.