2. Handlungsschritt (25 Punkte)

Die Sicherheit des Netzwerks der FUX AG soll durch verschiedene Maßnahmen verbessert werden.

a) Zur Verbesserung der Netzwerksicherheit wurde eine Firewall-Appliance integriert.

aa) Für den Datenverkehr in das Internet und vom Internet sollen unsichere, unverschlüsselte Protokolle gesperrt werden.

Ergänzen Sie die Tabelle um drei weitere unsichere Protokolle. 6 Punkte

Port	Protokoll	Beschreibung
25	SMTP	Mailversand
20/21	FTP	Dateitransfer
23	Telnet	Remote-Konsole
53	DNS	Domain-Name-Service – Namensauflösung
80	HTTP	HyperText Transfer Protokoll – Webseiten unverschlüsselt
110	POP3	Abholen von Mails beim Provider
79	Finger	Abfragen von Informationen
143	IMAP	Mail Management

Weitere Lösungen möglich.

ab) Im Funktionsumfang der Firewall-Appliance ist ein Virenscanner enthalten.

Erläutern Sie, warum eine Aktivierung des Virenscanners bei verschlüsselten Protokollen keine Verbesserung der Netzwerksicherheit bewirkt. 3 Punkte

Virenscanner können nur unverschlüsselte Daten nach Schadsoftware untersuchen.

ac) In der Firewall-Appliance ist ein IDS (Intrusion Detection System) integriert.

Beschreiben Sie anhand von zwei Aspekten, warum es sinnvoll ist, auch das interne Netz durch ein IDS zu überwachen. 4 Punkte

Ein IDS ist ein System, das Angriffe und andere Auffälligkeiten im Netzwerk erkennt.
Schadsoftware kann über verschlüsselte Verbindungenbei Download oder durch Datenträger wie USB-Sticks ins interne Netzwerk gelangen. Ein IDS könnte auffälligen Datenverkehr entdeckenund Gegenmaßnahmen veranlassen bzw. den Administrator informieren.
Weitere Lösungen möglich.

b) Die Netzwerk-Ports in den Büros sollen gegen das Anschließen unternehmensfremder Rechner geschützt werden.

Beschreiben Sie eine Möglichkeit, wie nur unternehmenseigenen Rechnern der Zugang zum Netzwerk erlaubt werden kann. 4 Punkte

- (Port Security) Die Switch-Ports werden eine Zeit lang in einen Lernmodus versetzt. Der Switch merkt sich alle (am Port) angeschlossenen Hardwareadressen (MAC) der Geräte. Dann werden die Switch-Ports in den „Security“-Modus gesetzt. Wenn nun ein Gerät mit neuer Hardwareadresse angeschlossen wird, kennt der Switch dieses Gerät nicht und sperrt den Port.
- (RADIUS) Die unternehmenseigenen Rechner sind mit ihrer MAC-Adresse in einer Datenbank hinterlegt. Über einen Radius-Dienst wird nun die MAC-Adresse eines angeschlossenen Rechners mit der Datenbank überprüft. Ist diese MAC nicht enthalten, wird der Port gesperrt bzw. nicht freigeschaltet.

Weitere Lösungen möglich.