Computertechnik

Die Aufgaben dienen der Vorbereitung auf die Gesellenprüfung. Sie festigen den Lehrstoff während der Ausbildung und unterstützen die Erarbeitung der Lernfelder 1–8. Lösungsvorschläge finden Sie auf Seite 16.

1 Rechnernetze
Firewall

LF 1 2 3 4 5 6 7 8

Vor Angriffen aus dem Internet werden Einzel-PCs und lokale Netzwerke durch sogenannte Firewalls geschützt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) liefert zur Erklärung dieses Begriffes folgende Umschreibung: „Eine Firewall dient zur Kontrolle der Kommunikation zwischen zwei Netzen. Im Regelfall wird sie zum Schutz eines Netzes gegen Angriffe aus dem Netz mit einem geringeren Schutzbedarf eingesetzt, ...“. Als Firewall wird eine Kombination von Hard- und Software bezeichnet, die als alleiniger Übergang zwischen zwei zu trennenden TCP/IP-Netzen dient“. Da Firewalls vorzugsweise zum Schutz vor Angriffen aus dem Internet eingesetzt werden, ist auch der Begriff Internet-Firewall gebräuchlich. Geht es lediglich um den Schutz eines einzelnen Personalcomputers, dann spricht man von einer Personal-Firewall. Firewalls bestehen aus verschiedenen Grundbausteinen.

Paketfilter. Die einfachste Möglichkeit zur Realisierung einer Firewall ist die Filterung der Datenpakete. Dazu können alle auf der Internet- und der Transportschicht verfügbaren Adressierungsinformationen genutzt werden. Hierzu gehören

- die IP-Adresse des Senders/Empfängers,
- der Protokolltyp und
- die Port-Nummer des Senders/Empfängers.

Da zur Formulierung der Filterregeln vorzugsweise die Port-Nummern verwendet werden, bezeichnet man Paketfilter zuweilen auch als Portfilter. Die Formulierung von Filterregeln muss getrennt für ankommende und abgehende Pakete erfolgen. Bezüglich der Leistungsfähigkeit von Paketfiltern wird zudem zwischen statischen und dynamischen Paketfiltern unterschieden. Dynamische Paketfilter passen Filterregeln aktuellen Systemzuständen automatisch an und sind daher flexibler einsetzbar.

Proxies. Ausgehend von der Tatsache, dass den im Internet angebotenen Diensten das Client-Server-Prinzip zugrunde liegt, werden Proxies („Stellvertreter“) als drittes Element zwischen Client und Server angeordnet. Gegenüber dem Client nimmt der Proxy die Rolle des Servers ein, daher wird zuweilen auch von Proxy-Servern gesprochen. Gegenüber dem Server im Internet agiert der Proxy als Client. Softwareseitig können Proxies sowohl auf der Transportschicht als auch auf der TCP/IP-Anwendungsschicht realisiert werden. Die auf der Anwendungsschicht arbeitenden Proxies werden auch als „Application Level Gateway“ bezeichnet. Hier wird für jeden Dienst ein gesonderter Proxy (z. B. HTTP-Proxy, SMTP-Proxy) installiert. Ein auf der Transportschicht arbeitender Proxy wird als „Circuit Level Gateway“ bezeichnet und kann zugleich mehrere Dienste der Anwendungsschicht bedienen. Neben der Kontrolle des Datenverkehrs wird durch den Einsatz eines Proxies auch eine Abschirmung des dahinter liegenden Netzes erreicht, da nach außen nur die IP-Adresse des Proxy sichtbar wird. Um den Proxy gegen Angriffe aus dem Netz zu schützen werden Maßnahmen ergriffen wie etwa

- Entfernen von Betriebssystembestandteilen oder
- Booten von Nur-Lese-Speichern (z. B. CD-/DVD-ROM).

Eine solcherart „gehärtete“ Station wird auch als „Bastion Host“ bezeichnet.

Adressumsetzung. Die Technologie der Adressumsetzung (NAT Network Adress Translation) ist wegen der begrenzten Verfügbarkeit von IP-Adressen entwickelt worden. Mit der Adressumsetzung können Netze in denen private IP-Adressen verwendet werden mit dem Internet verbunden werden. In diesem Fall bekommt lediglich der an der Grenze zwischen dem privaten Netz (LAN) und dem Internet angeordnete Router eine öffentliche IP-Adresse vom Provider zugewiesen. Die Zuordnung von internen und externen Verbindungen erfolgt über eine Tabelle unter Nutzung der Port-Nummern.

a) Was wird mittels IP-Adressen adressiert und auf welcher Schicht erfolgt dies?

b) Was wird mittels Port-Nummern adressiert und auf welcher Schicht erfolgt dies?

c) Was verstehen Sie unter dem Client-Server-Prinzip?

d) Welche IP-Adressbereiche stehen für private Netze jedermann zur Verfügung? Was passiert, wenn ein Paket mit einer privaten IP-Adresse aus dem LAN ins Internet gelangt?

e) Was verstehen Sie unter einem Screening Router? Skizzieren Sie die Anordnung und beurteilen Sie dessen Schutzwirkung. Wodurch wird die Schutzwirkung erhöht?



