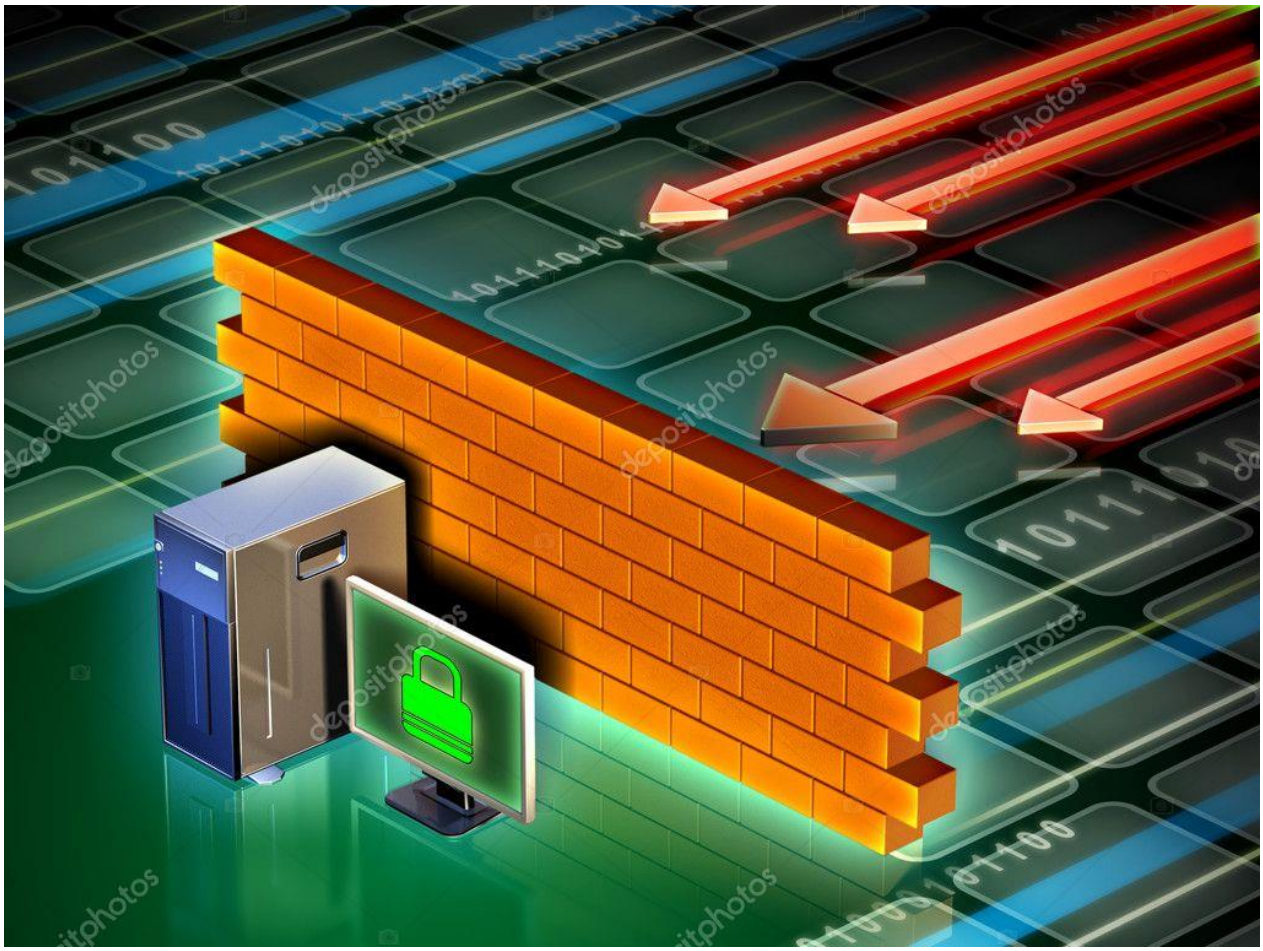
Sicherheit



Quelle: https://static8.depositphotos.com/1005669/1005/i/950/depositphotos_10052351-stock-photo-computer-firewall.jpg

Modul SC
Modulunterlagen

Inhaltsverzeichnis

Identifikation und Änderungsgeschichte

Dokumenttitel:	Modulunterlagen
Thema:	Modul SC Sicherheit
Autor:	Patrick Kramer
Firma:	RAU, Regionales Ausbildungszentrum Au
Dateiname:	HandOut-SC_Sicherheit_v10
Ablageort:	K:\Module_ab_2021\SC_Sicherheit\Lernende\HandOut-SC_Sicherheit_v10.docx
Druckdatum:	21.03.2022

Version	Datum	Bemerkungen
1.0	Februar 2022	Initialversion / PK

1 Handlungsziele und Handlungsnotwendige Kenntnisse

Quelle: ICT-Berufsbildung Schweiz

Titel		**Sicherheit**
Kompetenz		Massnahmen anhand von Sicherheitsaspekten ableiten.
Handlungsziele	1.	Kennt Sicherheitsrelevante Gefahren aus Sicht des Anwenders.
	2.	Kennt die Funktion und die wichtigsten Header-Felder der Protokolle eines IP Netzes (Ethernet, IP, ARP, ICMP, TCP, DHCP, DNS) und kann aufzeigen, welchen Beitrag diese zu einem funktionsfähigen Netzwerk leisten.
	3.	Kennt die häufigsten Fehler in den OSI Layers 2-4 und kann die dazugehörigen Symptome beschreiben.
	4.	Kennt Methoden und Werkzeuge zu Analyse der Protokolle und Abläufe (Protocol Analyser, Netzwerkmonitor) und kann aufzeigen, welche Arten von Fehlern mit diesen Methoden und Werkzeugen aufgedeckt werden können.
	5.	Überwachen von Komponenten.

Handlungsnotwendige Kenntnisse beschreiben Wissenselemente, die das Erreichen einzelner Handlungsziele eines Moduls unterstützen. Die Beschreibung dient zur Orientierung und hat empfehlenden Charakter. Die Konkretisierung der Lernziele und des Lernwegs für den Kompetenzerwerb sind Sache der Bildungsanbieter.

2 Einführung

2.1 Über dieses Dokument

Beim vorliegenden Dokument handelt es sich um ein Aufgabenskript mit Fragen und Querverweisen auf weiterführende Quellen.

Dieses Modul setzt gewisse Kenntnisse und Kompetenzen im Zusammenhang mit dem Aufbau und Betrieb von Client-/Server-Umgebungen voraus.

Folgender Hinweis kann bei einzelnen Aufgaben auf Kapitel in bestimmten Referenzen aufmerksam machen, die zum Lösen der entsprechenden Aufgaben besonders hilfreich sind:

	**Wikipedia**	Referenz auf ein bestimmtes Thema.

2.2 Über die Methodik

Tipp

Die Aufgaben sind schrittweise aufgebaut. Die einzelnen Schritte werden erklärt oder demonstriert und können jeweils anschliessend praktisch trainiert werden.

Diese Arbeitsweise zieht sich durch das ganze Modul. Die Erklärungen sind sehr kurz gehalten. Maximal profitieren Sie dann, wenn Sie anhand der Referenzen Beispiele analysieren, diese nachvollziehen, abändern und selber weiterentwickeln.

3 Leistungsbeurteilung

3.1 Vorgaben

Gewichtung in %	100
Beschreibung	Erarbeitete Lösungen werden auf dem Prüfungsbogen notiert. Um den Korrekturaufwand gering zu halten sind kurze Antworten gefordert.
Hilfsmittel	Unterlagen und persönliche Notizen aus dem Modulunterricht
Bewertungskriterien	Netzwerke mit geeigneten Tools ausmessen (20 - 30%)
	Netzwerkanalyse (20 – 30%)
	Dienste im Netz erkennen (15 – 25%)
	Sicherheitsaspekte erkennen und Massnahmen vorschlagen (15 - 25%)

4 Einleitung

Es bestehen grosse Unterschiede zwischen einer privaten und einer geschäftlichen Nutzung von IT-Infrastruktur. Der Ihnen im RAU zur Verfügung gestellte Rechner…..

- Unterschiede private geschäftliche Nutzung?
- Wieviel Geld steckt in der Anschaffung und im Unterhalt eines einzelnen Arbeitsplatzrechners?
- Was bedeutet dies für ein Unternehmen?
- Reglungen Gebrauch von IT-Mitteln?
- Welche Regeln würden Sie aufstellen, wenn verantwortlich für 4 bis 5 Arbeitsstationen? Internet abschalten?
- Individualisierung ist trotzdem möglich!
- Diskussion/Fragen beantworten in Partnerarbeit. Resultate in Dokument festhalten. (Dokument wieder verwendbar als Ausgangslage Textverarbeitung). Auswertung im Plenum
- Das persönliche Handy aufladen?

4.1 Client Security

Es folgen verschiedene Fragen zum Thema Security. Sie sollen die Grundlagen für eine aktive Diskussion schaffen, bei der alle bezüglich der Security und möglichen Massnahmen sensibilisiert werden.

4.1.1 Allgemeine Diskussion und Fragen

[F1]	Was ist Malware?
[F2]	Welche Arten von Malware existieren oder welche Ziele werden damit verfolgt?
[F3]	Wie verbreitet sich Malware?
[F4]	Welche Malware oder welche Art von Malware ist gerade sehr aktuell?
[F5]	Was waren Ihrer Meinung nach die schwerwiegendsten Sicherheitslücken der letzten Jahre?
[F6]	Welche weiteren Begriffe bezüglich Malware und Security kennen Sie oder wollen Sie besser kennen lernen?
[F7]	Wie infiziert denn Malware einen PC?
[F8]	Wie kann man sich vor Malware schützen?
[F9]	Kennen Sie andere spezielle Geschichten oder Angriffe aus IT Security?

[F10]	Was konnten Sie bis jetzt noch nicht sagen?	
[F11]	Wie funktioniert Anti Viren Software überhaupt?	
	**Web**	http://www.melani.admin.ch

4.1.2 Präsentation Virus

Um uns genauer mit Schadsoftware auseinander zu setzen hält jede Gruppe eine kurze Präsentation über eine Schwachstelle bzw. einen Virus.

A1	Dauer: 5min. Vorbereitungszeit: 1h Minimaler Inhalt: • Genutzte Sicherheitslücke / Technische Beschreibung • Entdeckung • Auswirkungen • Gegenmassnahmen und Prävention

4.2 Sicherheit bei Netzwerkkomponenten

Im vorherigen Kapitel wurden Sie hinsichtlich Client Security sensibilisiert. In einer produktiven Umgebung haben Sie neben Clients und Servern noch Netzwerkkomponenten.

[F1]	Warum sind Updates auf Computern (Clients & Servern) so wichtig?
[F2]	Welche Erkenntnis ziehen Sie aus der vorherigen Frage für Ihre Netzwerkkomponenten, welche Sie privat im Einsatz haben?

4.3 Datenschutz

F1	Grundrecht auf Datenschutz „*Jede Person hat das Recht, über die Weitergabe und Verwendung ihrer persönlichen Daten zu bestimmen (informationelles Selbstbestimmungsrecht).*“ Ich sniffe am Netzwerk und schaue die privaten E-Mails meiner Mitlernenden an. Zudem klaue ich das Passwort für den Mailzugriff von Tobias. Mache ich mich strafbar (mit Begründung)? Wenn ja, warum? Darf ich mit dem Passwort die Mails von Tobias anschauen? Ich lasse alles so wie es ist und verändere nichts.
A1	Der Datenschutz ist immer eine heikle Frage in der Netzwerkanalyse. Welche Daten dürfen Sie analysieren. Welche Vorkehrungen müssen Sie treffen, damit Sie die Daten im Netzwerk analysieren können. Wo ist der Unterschied zwischen legal und Illegal?

5 Netzwerkanalyse

5.1 Thema und Zielsetzung

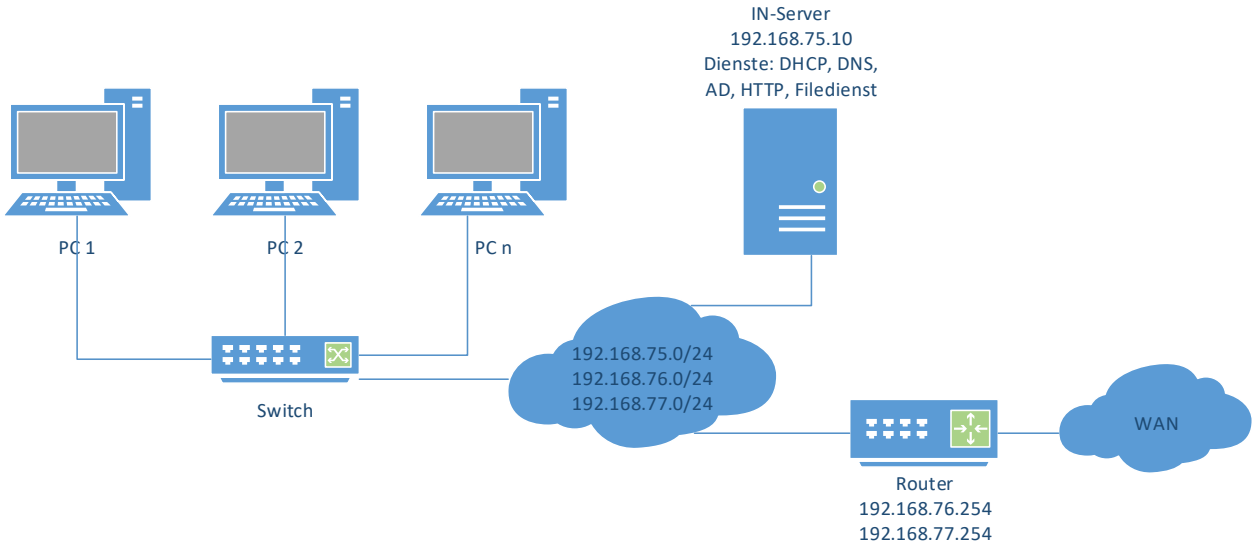
In den folgenden Aufgaben wird der Einsatz eines Netzwerk-Sniffers resp. Protokoll-Analyzers am Beispiel von *Wireshark* trainiert. Damit werden folgende Zielsetzungen verfolgt:

- Möglichkeiten und Grenzen von Sniffern kennen
- Sniffer und dessen Filter situationsgerecht und ressourcenschonend einsetzen
- Kenntnisse und Verständnis verschiedener Netzwerkprotokolle vertiefen
- Bewusstsein bezüglich der Sicherheit in Netzwerken wecken

5.2 Hilfsmittel

Hardware	• PC mit Netzwerkanschluss (Ethernet oder WLAN)
Software	• *Wireshark*
Dokumente	• Wireshark User's Guide • Wireshark Wiki: https://wiki.wireshark.org

5.3 Testumgebung



5.4 Dokumentation der Lösungen

Führen Sie eine Liste mit allen Messungen, welche Sie im Rahmen der Aufgaben in diesem Kapitel aufzeichnen. Nummerieren Sie alle Messungen und speichern Sie die zugehörigen Dateien der Aufzeichnung (Capturefiles) ab. Halten Sie zusätzlich zu jeder Messung fest, welche Filtereinstellungen für die Aufzeichnung verwendet wurden.

5.5 Vorbereitung und Analyse der Testumgebung

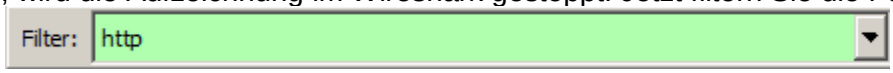
Bearbeiten Sie nun die folgenden Aufgaben:

A1 Installation Wireshark

Machen Sie sich mit der Dokumentation von Wireshark (www.wireshark.org) vertraut und installieren Sie das Tool. Wählen Sie das Interface für den LAN-Adapter aus und starten Sie die Aufzeichnung.

A2 TCP Stream Filter

Starten Sie eine neue Aufzeichnung.

Im Webbrowser öffnen Sie die Website www.r-au.ch. Wenn die Website vollständig angezeigt wird, wird die Aufzeichnung im Wireshark gestoppt. Jetzt filtern Sie die Pakete auf „HTTP“ 

Als Nächstes wird auf die Anfrage der Website gefiltert. Dazu wird das Paket mit der Info „GET / HTTP/1.1“ ausgewählt und mit der rechten Maustaste wählen Sie den Befehl „Follow TCP Stream“. Nun werden alle Requests und Response der Seite übersichtlich angezeigt. Der Filter wird wieder mit „Clear“ zurückgesetzt.

A3 IP Filter

Es werden drei Filter getestet. Was stellen Sie fest und wie verhält sich der Filter?

Filter	**Verhalten**
ip.addr==192.168.200.124	
ip.src==192.168.200.124	
ip.dst==192.168.200.124	

A4 Pakete suchen

Öffnen Sie eine Website und zeichnen Sie die Pakete in Wireshark auf. Anschliessend suchen Sie das Startpaket mit „GET“. Wie gehen Sie vor?

Wie wird diese Such-Funktion verwendet, um ein Passwort zu finden?

Nach „pw“, „pass“, „password“, „user“ oder „usr“ suchen. Falls der Username bekannt ist, dann direkt nach dem Name suchen z.B. „cisco“, „admin“ usw.

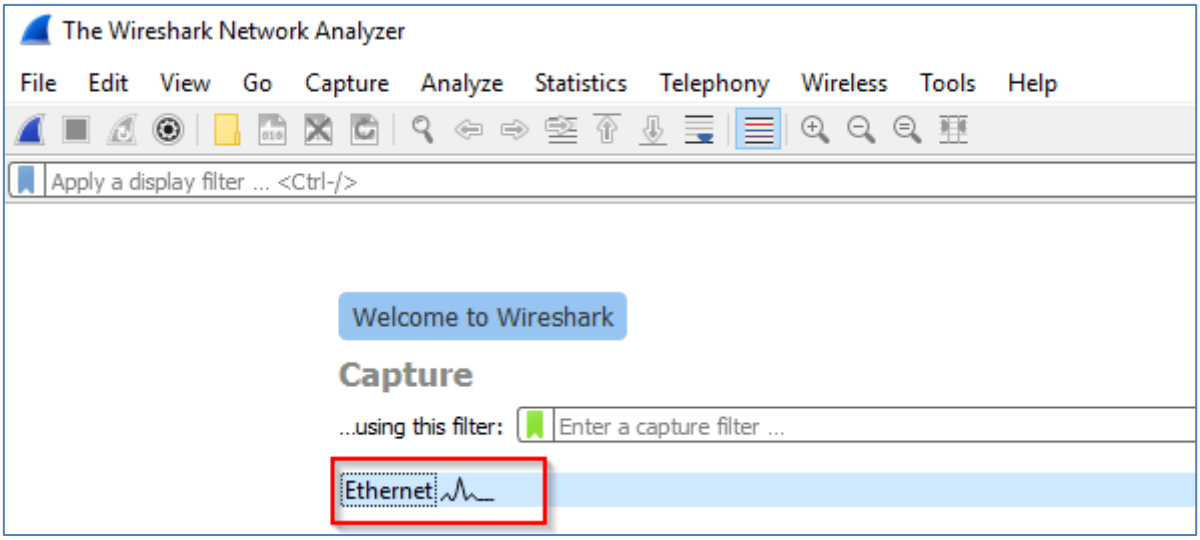
A5 Ermitteln Sie auf der Kommandozeile folgende Informationen:

DHCP ja / nein	
IP, Subnetmask	
Standardgateway:	
Server zur Namensauflösung:	

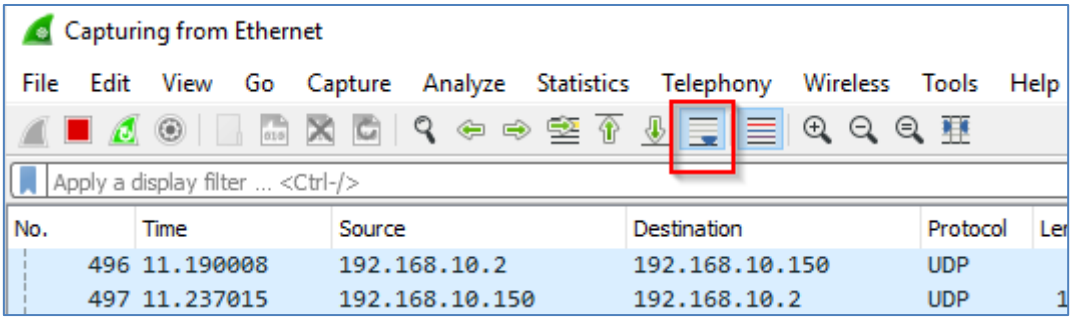
A6 Prüfen Sie die Funktion der Namensauflösung (DNS) mit dem Kommando *nslookup*. Notieren Sie Ihr Vorgehen und das Resultat.

5.6 Erste Schritte

Beenden Sie alle Applikationen (z.B. Browser, E-Mail, IP-Phone Client usw.) auf Ihrem PC, welche regelmässig über das Netzwerk kommunizieren. Öffnen Sie Wireshark und starten Sie eine Aufzeichnung des Netzwerkverkehrs, indem Sie im Startbildschirm einfach den entsprechenden Netzwerk-Adapter auswählt:



Aktivieren Sie ebenfalls über den unten eingezeichneten Knopf das «Automatische Scrollen»



Lassen Sie die Aufzeichnung solange laufen, bis rund 100 Pakete aufgezeichnet wurden. Untersuchen Sie nun, von welchen Protokollen Pakete aufgezeichnet wurden und notieren Sie diese in der Tabelle auf der folgenden Seite. Formulieren Sie in der zweiten Spalte kurz, wozu die einzelnen Protokolle verwendet werden. Schreiben Sie nicht einfach, was die Abkürzung bedeutet. Informieren Sie sich bei Bedarf im Internet.

Protokoll	Kurze Beschreibung / Zweck

5.7 ICMP

ICMP wird in TCP/IP-Netzwerken zum Austausch von Fehler- und Informationsmeldungen verwendet. ICMP-Pakete werden z.B. auch bei einem *ping*-Kommando ausgetauscht.

Wählen Sie eine IP eines Rechners im LAN aus und nehmen Sie die nötigen Einstellungen vor, damit nur Pakete von und zu dieser IP aufgezeichnet werden. Zeichnen Sie nun den Verkehr bei einem *ping*-Kommando auf die ausgewählte IP auf.

A1	Mit welchem Capturefilter kann die Aufzeichnung des Netzwerkverkehrs auf eine einzige IP beschränkt werden?
A2	Welcher Typ eines ICMP-Pakets wird bei einer Anfrage verschickt?
A3	Welcher Typ eines ICMP-Pakets wird bei einer Antwort verschickt?
A4	Wie viele Bytes und welche Informationen werden im Datenteil mit einem *ping* standardmässig verschickt?
A5	Wie kann die Anzahl übertragener Bytes beim *ping* beeinflusst werden? Belegen Sie die Wirkung dieser Option mit einer zusätzlichen Messung.

5.8 ARP

Das Address Resolution Protocol ARP ist ein Netzwerkprotokoll für die Zuordnung von Netzwerkadressen (z.B. IP) zu Hardwareadressen (z.B. MAC-Adressen bei Ethernet). In dieser Aufgabe werden Pakete der ARP-Kommunikation aufgezeichnet und untersucht.

Überlegen Sie sich vor den Aufzeichnungen folgende Punkte:

A1	Die Zuordnung von IP- zu MAC-Adressen als Resultat einer ARP-Anfrage erfolgt im OS in einer sogenannten Übersetzungstabelle (ARP-Cache). Mit welchem Kommando kann der Inhalt dieser Übersetzungstabelle angezeigt werden?
A2	Welche Informationen werden im ARP-Cache gespeichert und wie lange bleibt diese Speicherung erhalten?
A3	Mit welchem Kommando kann der ARP-Cache vor einer Aufzeichnung gelöscht werden?
A4	Wie kann eine ARP-Kommunikation im Netzwerk bewusst ausgelöst werden?

Wählen Sie eine IP eines Rechners im LAN aus und nehmen Sie die nötigen Einstellungen vor, damit nur Pakete von und zu dieser IP aufgezeichnet werden. Stellen Sie zusätzlich sicher, dass der lokale ARP-Cache leer ist und zeichnen Sie danach den Netzwerkverkehr auf, wenn der entfernte Rechner mit einem *ping* aufgerufen wird.

A5	An welche MAC-Adresse (Ethernet) wird der ARP-Request verschickt?
A6	Welche Unterschiede gibt es beim Datenteil der ARP-Kommunikation zwischen der Anfrage (Request) und der Antwort (Reply)?

5.9 DHCP

Das Dynamic Host Configuration Protocol DHCP ermöglicht mit Hilfe eines entsprechenden Servers die dynamische Zuweisung von IP-Adresse und weiterer Konfigurationsparameter an Computer. In dieser Aufgabe werden Pakete der DHCP-Kommunikation aufgezeichnet und untersucht.

Überlegen Sie sich vor den Aufzeichnungen folgende Punkte:

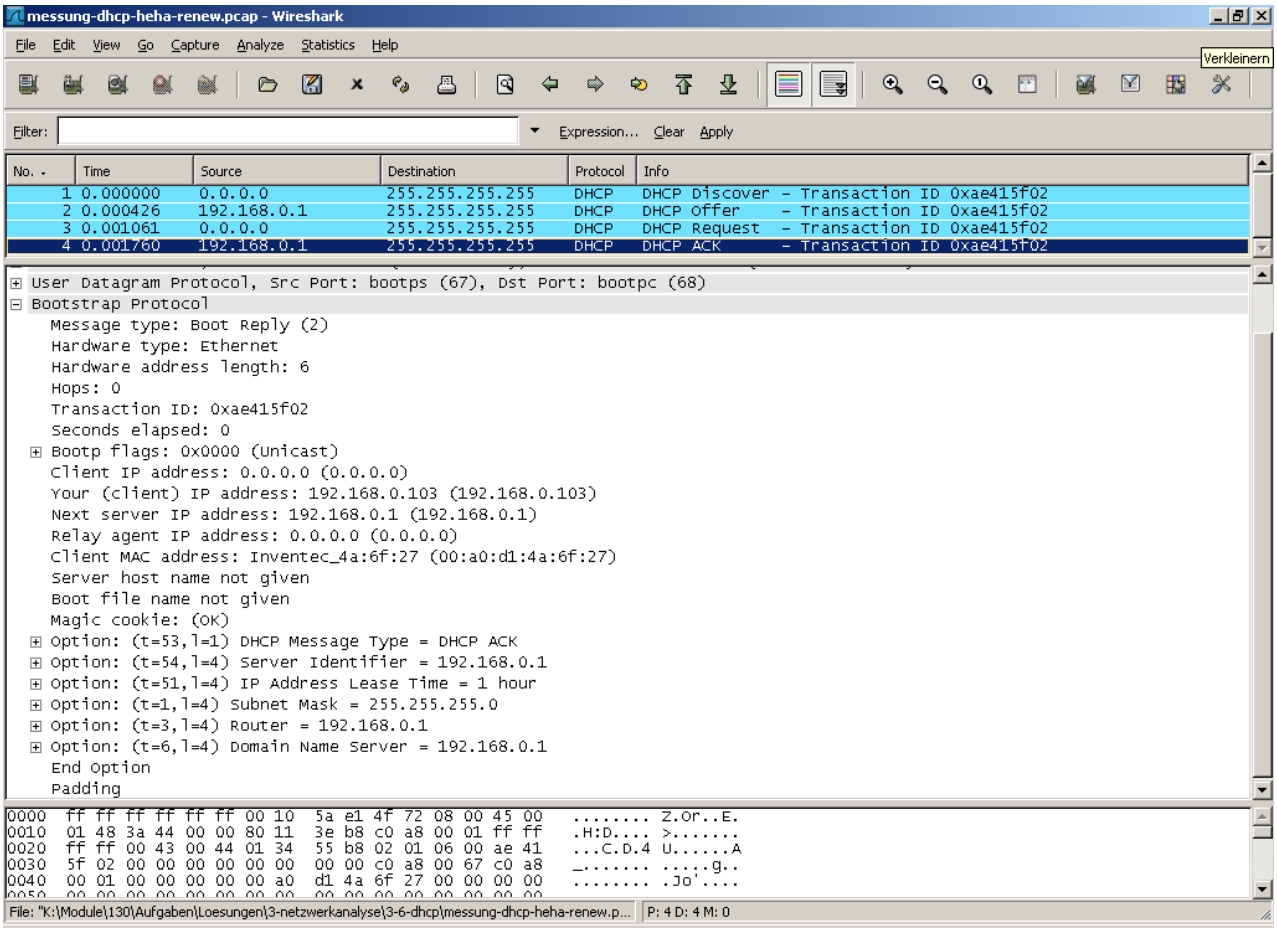
A1	Mit welchem Kommando kann der Bezug einer IP-Adresse von einem DHCP-Server resp. die Rückgabe der Adresse an einen DHCP-Server gesteuert werden?
A2	Welche Einstellungen müssen im Capturefilter von *Wireshark* vorgenommen werden, wenn nur DHCP-Pakete aufgezeichnet werden sollen? Hinweis: Überlegen Sie sich dazu, mit welchem Protokoll und auf welchem Port der DHCP-Server angesprochen wird.

Nehmen Sie die nötigen Einstellungen vor, damit alle DHCP-Pakete von und zum eigenen Rechner aufgezeichnet werden. Setzen Sie ein Kommando ab, damit die DHCP-Lease des Rechners an den Server zurückgegeben wird. Zeichnen Sie dann die Kommunikation auf, wenn beim DHCP-Server eine neue Lease angefordert wird.

A3	Wie viele Datenpakete umfasst die DHCP-Kommunikation zwischen Client und Server bei der Anforderung einer Lease? Überlegen Sie sich eine Eselsbrücke um sich den Ablauf besser zu merken.
A4	An welche IP adressiert der Client seine Anfrage und warum?
A5	An welche IP adressiert der Server seine Antwort und warum?
A6	Welche Werte sendet der Server dem Client für folgende Optionen?

Leasedauer	
Erneuerungszeit (Renewal Time)	
Serveridentifikation	
Subnetmaske	
Standardgateway (Router)	
Domain Name	
DNS-Server	

Bis jetzt wurde das Verhalten des DHCP-Dienstes des Windows-Servers aufgezeichnet. Die Leistungsfähigkeit bezüglich den Optionen, d.h. welche Informationen den Clients mitgeteilt werden können, unterscheidet sich je nach eingesetztem DHCP-Server. Die folgende Aufzeichnung zeigt die Kommunikation mit einem *haneWin*-DHCP-Server.



A7	Welche Werte sendet der *haneWin*-DHCP-Server dem Client für folgende Optionen?	
	Leasedauer	
	Erneuerungszeit (Renewal Time)	
	Serveridentifikation	
	Subnetmask	
	Standardgateway (Router)	
	Domain Name	
	DNS-Server	
A8	Welche Unterschiede erkennen Sie zwischen dem Windows- und dem *haneWin*-DHCP-Server?	

5.10 SMB

Das SMB-Protokoll (Server Message Block) definiert verschiedene Kommunikationsbefehle, welche die Steuerung resp. Verwaltung von Ressourcen wie Dateisysteme oder Drucker im Netzwerk ermöglichen. Das SMB-Protokoll läuft unter Windows als Dienst *microsoft-ds* auf Port 445 über TCP und UDP.

Richten Sie auf einem entfernten Rechner im LAN ein Verzeichnis ein und geben Sie dieses frei. Erstellen Sie in diesem Verzeichnis ein Textfile mit Ihrem Namen. Zeichnen Sie nun die SMB-Pakete auf, welche beim Zugriff auf das freigegebene Verzeichnis und beim Öffnen resp. beim Schliessen der Textdatei ausgetauscht werden.

A1	Können Sie den angeforderten Dateinamen in einem Paket finden? Mit welchem SMB-Befehl wird die Datei auf dem Client geöffnet?
A2	Mit welchem SMB-Befehl wird die Datei geschlossen?

Zeichnen Sie einen Druckauftrag auf einen Netzwerkdrucker Ihrer Wahl auf.

A3	Können Sie den Dateinamen der gedruckten Datei in einem Paket finden?
A4	Können Sie den Druckernamen in einem Paket finden? Geben Sie dabei den Druckernamen Ihrer Aufzeichnung an.

5.11 DNS

Das Anwendungsprotokoll DNS wird bei der Kommunikation mit einem Domain Name Server verwendet, welcher Domainnamen in IP-Adressen auflöst. In dieser Aufgabe werden Pakete der DNS-Kommunikation aufgezeichnet und untersucht.

Überlegen Sie sich vor den Aufzeichnungen folgende Punkte:

A1	Mit welchem Kommando kann eine DNS-Abfrage gemacht werden?
A2	Wie verhalten sich DNS-Server, wenn eine Anfrage nicht beantwortet werden kann (Stichworte rekursive resp. iterative Suche)?
A3	Welche Einstellungen müssen im Capturefilter von *Wireshark* vorgenommen werden, wenn nur DNS-Pakete aufgezeichnet werden sollen? Hinweis: Überlegen Sie sich dazu, mit welchem Protokoll und auf welchem Port der DNS-Server angesprochen wird.

5.11.1 DNS-Anfrage nach Rechner im LAN

Zeichnen Sie alle DNS-Pakete zwischen Client und Server bei einer Anfrage nach einem lokalen Rechnernamen im LAN auf.

A4	Wie viele Pakete werden ausgetauscht bis der DNS-Server die Antwort liefert und was passiert dabei genau?

5.11.2 DNS-Anfrage nach Rechner im WAN

Zeichnen Sie nun die DNS-Kommunikation bei einer Anfrage nach einer Domain im Internet auf. Wählen Sie dazu bewusst eine unbekannte Domain, welche vom DNS-Server in letzter Zeit bestimmt nicht aufgelöst wurde.

A5	Wie viele Pakete werden nun ausgetauscht bis der DNS-Server die Antwort liefert und was passiert dabei genau? Beachten Sie dazu, welche DNS-Server als *authoritative nameservers* in der Antwort angegeben werden.
A6	Wiederholen Sie nun die Messung von oben und untersuchen Sie die Antwort. Wie begründen sich allfällige Unterschiede zur ersten Messung? Beachten Sie hier, ob überhaupt noch alternative DNS-Server in der Antwort angegeben werden.

5.11.3 DNS-Anfrage nach unbekanntem Rechner im WAN

A7	Zeichnen Sie nun die DNS-Kommunikation bei einer DNS-Anfrage für den fiktiven Rechner *a1b2c3d123.cn* in der Topleveldomain von China auf. Von welchem DNS-Server kommt die Antwort, dass dieser Name nicht vorhanden ist? Beachten Sie auch die im Vergleich zu den vorderen Messungen relativ lange Antwortzeit.

5.12 FTP

Das Anwendungsprotokoll FTP wird zur Übertragung von grösseren Datenmengen im Netzwerk (vor allem im Internet) eingesetzt. In dieser Aufgabe werden Pakete der FTP-Kommunikation aufgezeichnet und untersucht, wobei als FTP-Client sowohl der Browser (der auch einen FTP-Client enthält) wie auch der FileZilla-Client zum Einsatz kommen.

Die Eingabe der URL im Browser erfolgt nach dem Muster: ftp://user:password@adresse, wobei die Adresse sowohl eine IP oder ein Domainname sein kann. Bei vielen öffentlichen FTP-Servern handelt es sich um sogenannte Anonymous-Server, bei welchen keine Anmeldung erforderlich ist. Dann wird für den Benutzer *anonymous* eingegeben und das Passwort kann beliebig gewählt werden.

Überlegen Sie sich vor den Aufzeichnungen folgende Punkte:

A1	Welche Einstellungen müssen im Capturefilter von *Wireshark* vorgenommen werden, wenn nur FTP-Pakete aufgezeichnet werden sollen? Hinweis: Überlegen Sie sich dazu, mit welchem Protokoll und auf welchem Port der FTP-Server angesprochen wird.

Nehmen Sie die nötigen Einstellungen vor, damit alle FTP-Pakete von und zum eigenen Rechner aufgezeichnet werden. Zeichnen Sie dann die Kommunikation auf, wenn im Browser der anonyme FTP-Server unter ftp://speedtest.tele2.net (oder eine andere FTP-Seite) aufgerufen wird.

A2	Suchen Sie in den aufgezeichneten Paketen nach den Befehlen *user* und *pass*. Können diese gelesen werden?
A3	Suchen Sie in den aufgezeichneten Paketen nach der Antwort des Servers auf den Befehl *syst*. Wozu dient dieser Befehl offensichtlich und wie lautet die Antwort?

Zeichnen Sie jetzt die Kommunikation auf, wenn der gleiche Server mit dem FileZilla-Client aufgerufen wird. Beachte: Starten Sie den FTP-Client nur mit der Angabe der Adresse (ftp://speedtest.tele2.net) und geben Sie den Benutzer und das Passwort erst nach der entsprechenden Aufforderung des Servers an. So lassen sich die einzelnen Kommunikationsschritte im *Wireshark* gut beobachten.

A4	Wo finden Sie Unterschiede zwischen dem FTP-Client im Browser und dem installierten FileZilla-Client?
A5	Wird der Befehl *syst* auch vom FileZilla-Client übertragen und kann dieser Befehl manuell abgesetzt werden?

5.13 HTTP und HTTPS

Das **H**yper **T**ext **T**ransfer **P**rotocol HTTP dient hauptsächlich zur Übertragung von Webseiten von Webservern zur Darstellung im Browser des Clients. In dieser Aufgabe werden HTTP- und HTTPS-Pakete aufgezeichnet und untersucht.

5.13.1 Informationen im HTTP-Header

A1	Zeichnen Sie mit einem Aufruf auf eine beliebige http-Webseite auf, welche Informationen der Client im Header mit der GET-Methode bezüglich dem eingesetzten Browser und der bevorzugten resp. akzeptierten Sprache übertragen werden.
A2	Ermitteln Sie aus dem Header der HTTP-Response der folgenden Webseiten, welches Produkt und welche Version als Webserver eingesetzt wird. http://www.apache.org http://www.usz.ch
A3	Ermitteln Sie für die folgenden Webauftritte, ob die Server ein Caching der Seiten zulassen. Welche Felder im HTTP-Header beeinflussen das Caching und was ist der Unterschied zu den Metatag cache-control und expires innerhalb von HTML-Seiten? http://www.apache.org http://www.usz.ch

5.13.2 Übertragung von Formulardaten mit GET resp. POST

Benutzerdaten aus HTML-Formularen können unter HTTP sowohl mit der GET-Methode oder auch mit der POST-Methode an den Webserver übertragen werden. Der Unterschied liegt darin, dass die Daten bei der GET-Methode an die URL angehängt werden und damit im HTTP-Header übertragen werden, während die Formulardaten mit der POST-Methode im Datenteil des HTTP-Pakets übertragen werden. Dieser Unterschied soll mit den folgenden Aufzeichnungen illustriert werden.

Stellen Sie den Capturefilter von *Wireshark* so ein, dass alle Pakete zum und vom Webserver im LAN aufgezeichnet werden. Rufen Sie dann im M130-Webauftritt http://m130.r-au.ch die «Übertragung von Formulardaten» auf.

A4	Zeichnen Sie die HTTP-Kommunikation auf, wenn das ausgefüllte Formular einmal mit der GET-Methode und einmal mit der POST-Methode an den Server geschickt wird. Was ist in Bezug auf die Übertragung der Formulardaten zu beobachten?
A5	Was sind die Vor- und Nachteile der beiden Methoden? Welche Methoden werden in der Praxis sinnvollerweise wo eingesetzt?
A6	Können die vom Benutzer eingegebenen Formulardaten gelesen werden und wäre das auch so, wenn über HTTP ein Login mit Benutzername und Passwort übertragen würde?

5.13.3 Aufzeichnungen mit HTTPS

Nun wird die Kommunikation über HTTPS aufgezeichnet. Zeichnen Sie mit *Wireshark* ein Login auf den Webserver https://www.paypal.com/ auf. Dazu brauchen Sie sich nicht erfolgreich anzumelden, die Eingabe eines fiktiven Benutzers mit Passwort reicht für die Aufzeichnung des Requests.

A7	Welche Protokolle werden aufgezeichnet?
A8	Können Sie die eingegebene E-Mail-Adresse und das Passwort in den Nutzdaten finden?
A9	Zählen Sie einige Gründe auf, weshalb in der Praxis nicht ausschliesslich das sichere Protokoll HTTPS eingesetzt wird.

5.13.4 Analyse von Webmails

Auch die Daten von Webmails werden über HTTP oder HTTPS übertragen (und nicht über POP resp. SMTP). Für die Sicherheit ist es also entscheidend, welches Protokoll verwendet wird.

A10 Untersuchen Sie für die folgenden Webmail-Dienste, ob die Daten ab dem Login im Klartext oder verschlüsselt übertragen werden. Dazu brauchen Sie sich nicht erfolgreich anzumelden, die Eingabe eines fiktiven Benutzers mit Passwort reicht für die Aufzeichnung des Requests.

Adresse	https ja/nein	Besitzer-Information	Zertifikat ausgestellt für	Zertifikat ausgestellt von
www.bluewin.ch				
www.outlook.com				
www.gmx.ch				
www.gmail.com				

5.13.5 Messung des Overhead durch die Protokollheader

Jedes Protokoll fügt auf jeder Schicht im OSI-Modell zu den eigentlichen Nutzdaten zusätzliche Informationen zur Übertragung in Form von Protokollheadern hinzu. Diese Informationen sind zwar für die Übertragung notwendig, sind aber im Sinne von Nutzdaten für den Benutzer nutzlos. In dieser Aufgabe werden nun am Beispiel einer Webseite der Anteil der Steuer- und Nutzdaten genauer untersucht werden.

Stellen Sie den Capturefilter von *Wireshark* so ein, dass alle Pakete zum und vom Webserver im LAN aufgezeichnet werden. Rufen Sie unter dem M130-Webauftritt http://m130.r-au.ch die «Overheadmessung» auf.

A11	Zeichnen Sie die Antwort des Servers auf, wenn die *Seite 1* aufgerufen wird. Wenn alles rund gelaufen ist, bemerken Sie, dass diese kleine Seite mit nur einer HTTP-Response vom Server übertragen wurde. Füllen Sie nun die folgende Tabelle aus, indem Sie die Anzahl der übertragenen Bytes pro Protokollheader und die Nutzdaten aus der HTTP-Response ablesen resp. zählen.

OSI-Layer	Daten	Grösse in Bytes
1 und 2	Ethernet-Header	Bytes
3	IP-Header	Bytes
4	TCP-Header	Bytes
5 und 6	HTTP-Header	Bytes
7	Nutzdaten	Bytes
1 bis 7	Total	Bytes

A12	Berechnen Sie den prozentualen Anteil der Nutzdaten im Vergleich zum Total der übertragenen Bytes.

Zeichnen Sie nun das Verhalten bei einem HTTP-Request auf die *Seite 2* auf und beantworten Sie durch Analyse der Ergebnisse folgende Fragen:

A13	Wie viele HTTP-Requests werden vom Client abgesetzt, bis der ganze Inhalt der Webseite heruntergeladen ist? Begründen Sie Ihre Antwort.
A14	Wie reagiert der Webserver, wenn eine angeforderte Ressource (z.B. ein Bild) nicht in einer einzigen HTTP-Response übertragen werden kann?

Z1	Berechnen Sie den prozentualen Anteil der Nutzdaten. Beachten Sie dazu, dass auch die Bilder als Nutzdaten zu rechnen sind. Allerdings wird der Einfachheit halber dreimal das gleiche Bild geladen. Die Herleitung und der Nachvollzug der Rechnung muss ersichtlich sein.

5.14 Zusammenfassung

Sie haben nun etliche Messungen mit *Wireshark* gemacht und dabei auch gesehen, dass die Aufzeichnung von Datenpaketen aus der Sicht des Datenschutzes nicht unproblematisch ist. Abschliessend wollen wir zusammenfassend festhalten, wo sich der Einsatz eines Sniffers wie *Wireshark* in der Praxis lohnt und wo die Grenzen sind.

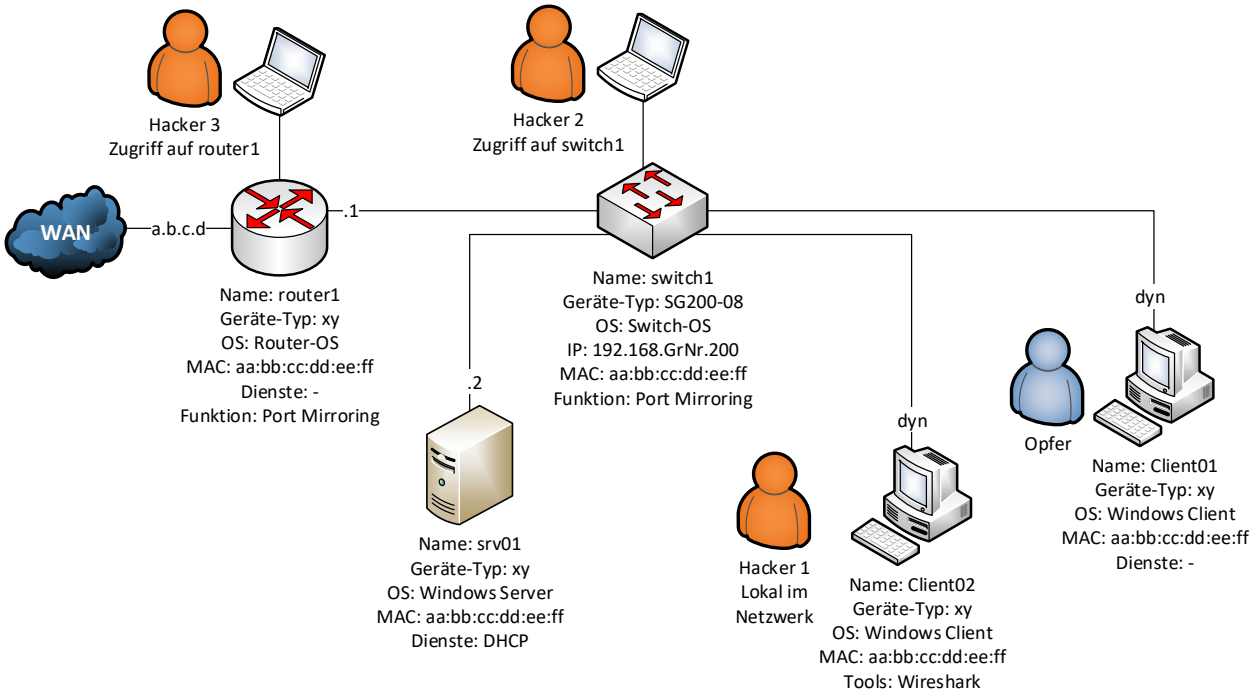
F1	Welche technischen Gegebenheiten können den Einsatz eines Sniffers (ohne zusätzliche Massnahmen) einschränken?
A1	Zählen Sie 5 praktische Problemstellungen oder Fehlersituationen auf, bei welchen sich der Einsatz eines Sniffers für die Lösung eignet resp. sinnvoll ist.

5.15 Hacker-Attack

In Hacker-Attack werden verschiedene Angriffspunkte im Netzwerk betrachtet. Es geht vorwiegend darum, die Schwächen eines Netzwerkes kennen zu lernen.

5.15.1 Netzaufbau

Bauen Sie folgendes Netzwerk auf:



A1	Konfiguration Switch SG200-08 Machen Sie sich mit dem Manual des Herstellers bekannt. Anschliessend konfigurieren Sie den Switch SG200-08. Es wird ein starkes Passwort zum Anmelden verwendet. Die IP des Switchs wird statisch auf 192.168.GrNr.200 gesetzt. Jetzt schliessen Sie den Hacker PC an und mittels „Port Mirroring“ werden die Pakete zum Hacker gespiegelt.
A2	Konfiguration Router Auf dem Router wird das „Port Mirroring“ für den Hacker-PC frei geschaltet.

5.15.2 Attack

A1	Opfer Das Opfer öffnet verschiedene Webseiten im Internet.
A2	Hacker 1 Versuchen Sie herauszufinden, auf welchen Seiten das Opfer surft. Was stellen Sie fest?
A3	Hacker 2 Versuchen Sie herauszufinden, auf welchen Seiten das Opfer surft. Was stellen Sie fest?

A4	Hacker 3 Versuchen Sie herauszufinden, auf welchen Seiten das Opfer surft. Was stellen Sie fest?
Z1	Portscanner Installieren Sie den Portscanner www.nmap.org. Starten Sie das Tool im lokalen Netzwerk und schauen Sie, welche Computer vorhanden sind. Vergleichen Sie die gemessenen Resultate mit Ihrem Netzplan.

5.15.3 Starke Passwörter

Im Modul NS haben Sie gelernt, was starke Passwörter ausmacht.

A1	Wie lautet die Formel, die für die Ermittlung der Stärke des Passworts herangezogen wird?

Wichtig

Jedes Zeichen soll möglichst zufällig sein. Kombinationen wie „1234“, „abcd“ oder „Wörter“ dürfen nicht verwendet. Sie sind (mit einem Wörterbuch) einfach zu hacken.

A2 Berechnen Sie die Kombinationen bei 12 Zeichen:

Symbole	Anzahl Symbole	Mögliche Kombinationen bei 12 Zeichen
A…Z	26	
A…Z, 0…9	36	
A…Z, a…z, 0…9	62	

A3 Schätzen Sie die Stärke der Passwörter ein:

Passwort	schwach	stark	Begründung
aaaaa	☐	☐	
aaaaaaaaaaaaaaa	☐	☐	
Raurau1234	☐	☐	
Los_angeles	☐	☐	
Lo$_@ngele$	☐	☐	
AznHu4Uv	☐	☐	
Ak15_p5cMp7!	☐	☐	

<table>
<tr><td>A4</td><td>Entwerfen Sie ein starkes Passwort anhand des Beispiels. Merken Sie sich die Eselsbrücke.<table><tr><th>Satz</th><th>Passwort</th></tr><tr><td>An meinem 18 Geburtstag war ich in New York – bäm</td><td>Am18GwiiNY-b</td></tr></table></td></tr>
<tr><td>A5</td><td>Wo werden ausschliesslich starke Passwörter verwendet?</td></tr>
</table>

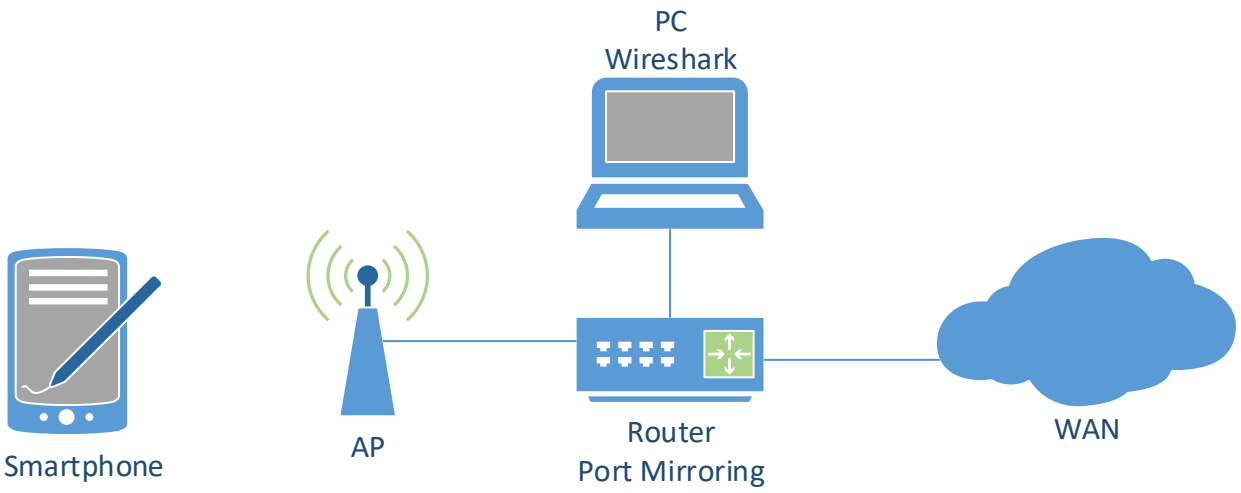
5.16 Smartphone App Analyse

5.16.1 Ausgangsituation

Auf den Smartphones können diverse Apps installiert werden. Diese Apps können heimlich die Userdaten aufzeichnen und an einen Server schicken. Dabei kann es sich um GPS-Daten, Telefonbucheinträge, Lieblingsnummern, usw. handeln. Die Daten werden meistens zu Werbezwecken analysiert. Damit ist es möglich, gezielt persönliche Werbung auf dem Telefon zu platzieren. Es werden Userprofile erstellt. Wenn Sie also dreimal in der Woche ins Starbucks gehen, so ist die Wahrscheinlichkeit gross, dass z.B. Google Werbeinserate von weiteren Kaffeeshops anbietet.

5.16.2 Messaufbau

Das Smartphone wird isoliert. Über einen Access Point (AP) wird das Telefon am WAN angeschlossen. Der Sniffer-PC wird mit dem Router verbunden. Dieser kann über Wireshark den gesamten Traffic des Smartphone mittels Port Mirroring mitlesen.



5.16.3 Messungen

A1	Bauen Sie die Test-Infrastruktur auf und öffnen Sie auf dem Smartphone eine Website. Fangen Sie diese mit dem Wireshark ab und speichern Sie das Capture-File. Ist der Test erfolgreich, können Sie mit der nächsten Analyse starten.
A2	Analysieren Sie den Datenverkehr des Smartphones. Was läuft im Hintergrund? Protokollieren Sie die Ergebnisse in einem Messbericht.

6 Informationssammlung

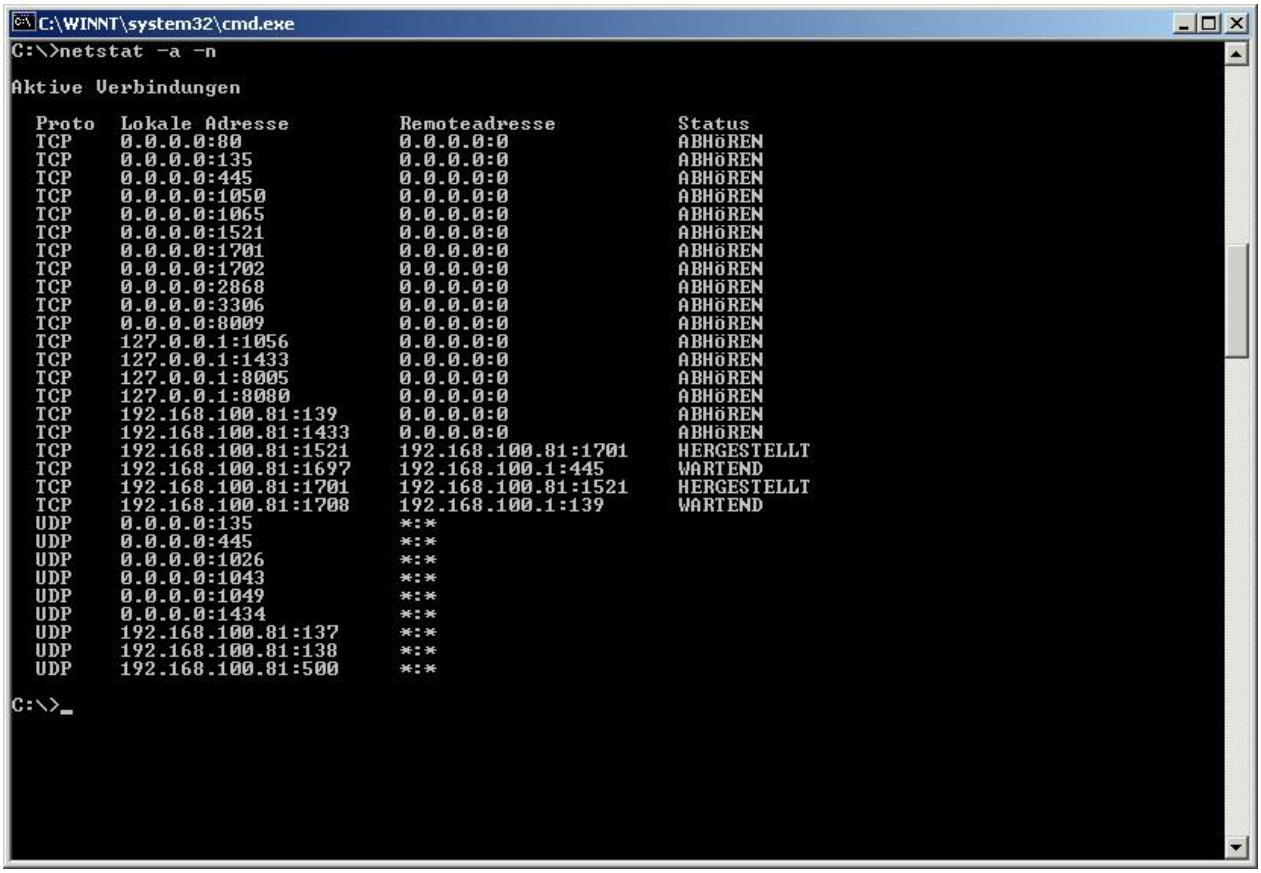
6.1 Portscan

A1	Ermitteln Sie mit *portqry* unter Windows die offenen Ports auf dem lokalen Rechner (nur well known ports). Was stellen Sie fest?
A2	Ermitteln Sie unter Windows mit *nmap* die offenen Ports der einzelnen Computer. Schauen Sie die Rechner und die Dienste an.
A3	Scannen Sie mit *nmap* einen entfernten Windows-Rechner mit eingeschalteter Firewall. Wird der Portscan durch die Firewall verhindert oder erkannt? Beachten Sie dazu auch die Logdatei der Firewall!
A4	Verifizieren Sie die Resultate von *nmap* mittels *netstat* auf einem entfernten Rechner. Kann *netstat* auf entfernte Rechner angewendet werden? Werden mit *netstat* noch weitere offene Verbindungen angezeigt?
Z1	Erstellen Sie ein Power Shell Skript, welches mit Hilfe von Ping einen Portscann durchführt. Wo finden Sie das Resultat? Geben Sie das Skript und das Resultat ab unter \Abgaben\RAU-Module\SC\Scan\Nachname Vorname\Nachname-Vorname.[Dateiendung]

6.2 Interpretation einer Ausgabe mit *netstat*

Die folgende Abbildung zeigt die Ausgabe des Kommandos *netstat* auf einem Rechner.

A1	Interpretieren Sie die Ausgabe und erstellen Sie eine Liste mit allen Diensten, welche wahrscheinlich auf dem Rechner aktiv sind. Informieren Sie sich bezüglich den Portnummern im Internet (de.wikipedia.org/wiki/Liste_der_standardisierten_Ports).



6.3 Social Engineering

In der Praxis gibt es manchmal Fälle, in welchen man Informationen über den Urheber einer Übertragung bestimmen möchte. Das kann zum Beispiel zur Ermittlung des Urhebers eines registrierten Portscans oder eines anderen Angriffs sein oder aber zur Gewinnung von Informationen bezüglich einem Absender einer E-Mail. Mit einem Phishing-Mail wird versucht an die Zugangsdaten des Users heranzukommen. Diesem Verfahren sagt man *Social Engineering*.

A1	Studieren Sie den Artikel Social Engineering de.wikipedia.org/wiki/Social_Engineering_(Sicherheit) und machen Sie sich mit dem Thema vertraut.
A2	Lösen Sie den Phishing-IQ-Test (sonicwall-phishing-iq-test) und definieren Sie zwei Killer-Kriterien mit denen Sie ein Phishing-Mail enttarnen können.

7 Monitoring

Das Ziel von Monitoring Systemen ist es, den Betrieb sicherstellen zu können und Kosten inkl. Ausfälle zu verhindern. Es geht darum nicht nur auf Fehler reagieren zu können, sondern mögliche Fehlerquellen frühzeitig zu erkennen.

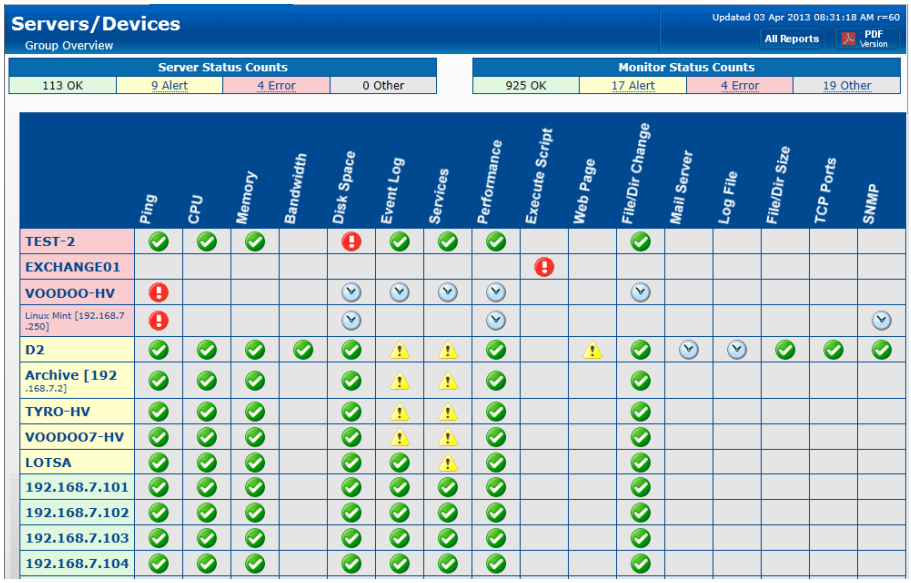


Abbildung 1: Monitoring-System

7.1 Messwerte

Zuerst muss man wissen, welche Werte eignen sich, um Server zu überwachen. Definierte Grenzwerte werden dabei vor allem für das Performance Monitoring genutzt. Um die Sicherheit und den Zustand eines Systems zu erkennen, werden jedoch die verschiedensten Logfiles eingesehen.

Wichtig ist zu wissen, dass nicht nur „ALARM“ und „alles OK“ gibt. Es können verschiedene Grenzwerte mit verschiedenen Eskalationsstufen definiert werden. Dazu benötigt man ein gutes Verständnis für die Applikation oder den Dienst, die auf einem System läuft.

7.1.1 Logfiles

Verschiedenste Ereignisse und Informationen können aus Logfiles gelesen werden. Es ist wichtig diese zu überwachen und zu alarmieren. Eine manuelle Kontrolle dieser Files ist kaum möglich, da die Datenmenge schlicht zu gross ist. Welche Informationen sich in einem Logfile befinden, und welche Logfiles überhaupt existieren, ist von Betriebssystem und den verwendeten Applikationen abhängig. Zusätzlich kann bei den meisten Applikationen ein Log-Level definiert werden.

Typische Log Level:

- ERROR / CRITICAL
  - Ereignisse, welche den ordentlichen Betrieb verhindern
- WARNING
  - Ereignisse, welche den ordentlichen Betrieb verhindern könnten

- INFO
  - Ereignisse, welche über den Zustand eines Systems Auskunft geben
- DEBUG
  - Informationen für Entwickler über das Verhalten der Applikation

Mögliche Ereignisse die aus Logfiles gelesen werden können:

- Zugriffe und Anfragen
  - Logins in das OS oder in Applikationen
  - Auch abgelehnte Versuche
- Verarbeitungsfehler
  - Dateien die nicht geschrieben werden konnten
  - Daten welche falsche im falschen Format gespeichert sind

7.1.2 Weitere Möglichkeiten

Zusätzlich zu Logfiles und der Performance können noch viele weitere Informationen in ein Monitoring System einfliessen. Diese Informationen beziehen sich oft auf eine Applikation oder ob ein System läuft und verfügbar ist oder nicht.

Nicht abschliessende Liste dieser Möglichkeiten:

- Ping
  - Erhalten wir eine Antwort des Systems
- Dienste und Prozesse
  - Sind die von uns erwarteten Prozesse am Laufen
- Eigene Scripts
  - Ist es möglich ein eigenes Script auszuführen
- Applikationsbezogen
  - Webseite kann ausgeliefert werden
  - Datenbank Login und Query sind möglich
  - DNS-Abfrage gibt korrekten Wert zurück

7.2 Monitoring Tools

Es gibt diverse Produkte für Monitoring-Lösungen. Einige bekannte Produkte sind Nagios, Microsoft System Center oder PRTG

7.2.1 Funktionsumfang

Ziel dieser Tools ist es den aktuellen Systemstatus der diversen Systeme einfach und übersichtlich darzustellen. Meistens wird dafür ein Webinterface benutzt.

Weiter ist es wichtig, dass man auf Fehler und Ereignisse schnell reagiert. Deshalb bieten Monitoring-Tools die Möglichkeit den Betreiber eines Systems zu alarmieren. Dies geschieht mit SMS, E-Mails oder sogar Anrufen. Dafür braucht es jedoch oft zusätzliche Software.

7.2.2 Funktionsweise

Einfach erklärt besteht das Monitoring System vielfach aus einem oder mehreren Servern und Agents, welche auf die zu überwachenden Systeme verteilt werden.

Die Agents führen auf den verschiedenen Systemen die Messungen durch und senden die Resultate an den Server. Dieser Sammelt die Informationen, stellt sie dar und zeigt entsprechende Warnungen und Alarme.

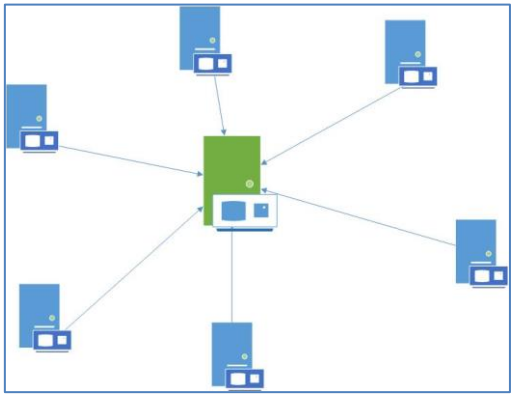


Abbildung 2: Aufbau Monitoring mit Agents

8 Fehlersymptome/–meldungen

8.1 Fehleranalyse

8.1.1 Einführung

Nachfolgend finden Sie eine kleine Auswahl an Werkzeugen, die Ihnen bei der Fehleranalyse zur Verfügung stehen.

Ereignisanzeige Windows

Die Ereignisanzeige ist die zentrale Anlaufstelle für Meldungen und Fehler im Betriebssystem und weist mindestens die Protokolle mit der Bezeichnung **Anwendung, System** und **Sicherheit** auf. Die Ereignisse sind in die drei verschiedenen Typen **Information, Warnung und Fehler** unterteilt.

Protokolldatei „syslog“ unter Linux

Unter Linux führt der Dienst **syslogd** die Ereignisprotokollierung durch. Sämtliche Protokolldateien befinden sich im Normalfall im Verzeichnis **/var/log/**. Eine zentrale Rolle spielt in diesem Zusammenhang die Datei „**syslog“,** welche grundlegende Ereignisse und Systemfehler protokolliert.

Ende der Protokolldatei anzeigen: ***tail /var/log/syslog***

Fortlaufend das Ende der Protokolldatei auflisten: ***tail –f /var/log/syslog***

A1	Überprüfen Sie die Ereignisanzeige unter Windows. Provozieren Sie im System einige Logs (Warnungen, Fehler).
A2	Überprüfen Sie nun die Datei **syslog** unter Linux. Provozieren Sie wieder Logeinträge.

8.2 Logserver

8.2.1 Einführung syslog

Syslog ist ein weit verbreiteter Standard für die Übertragung von Logdaten im Netzwerk. Der syslog-Dienst sendet und empfängt Nachrichten, kann also im Normalfall die Rolle eines Client- beziehungsweise eines Server-Programms einnehmen. Die Meldungen werden zum Zeitpunkt der Protokollierung mit einem **Zeitstempel**, dem **Priority-Code (Zusammensetzung von Facility und Severity)** und einer **Textmeldung** versehen. Durch die richtige Auswertung der Logdaten ist so das frühzeitige Erkennen von Fehlerverhalten möglich.

Syslog empfängt standardmässig Nachrichten vom Sender über den **UDP Port 514**. Die Meldungen werden im Klartext übertragen.

In hochwertigeren Netzwerkgeräten (Cisco, HP, Netgear) ist ein syslog-Agent im Normalfall schon integriert. Für die meisten Betriebssystemplattformen (Linux, Windows, Mac) gibt einen entsprechenden Agenten. Oft ist dieser sogar Bestandteil des Betriebssystems.

8.2.1.1 Facility

0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16 – 23	local use 0 - 7

Quelle: http://www.kiwisyslog.com/help/syslog/index.html?protocol_priority_values.htm

8.2.1.2 Severity-Levels

Code	Bezeichnung
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational
7	Debug

8.2.1.3 Konkretes Beispiel

```
<34>Oct 11 22:14:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8
```

A1	Die Logs eines Switches sollen auf den vorhandenen Linux-Server geschickt werden. Auf dem verwaltbaren wird *Remote Log Server* aktiviert und auf Ubuntu *rsyslog.conf* (*/etc/rsyslog.conf*) folgendermassen konfigurieren: UDP Port 514

9 Firewall

	Wikipedia	Firewall

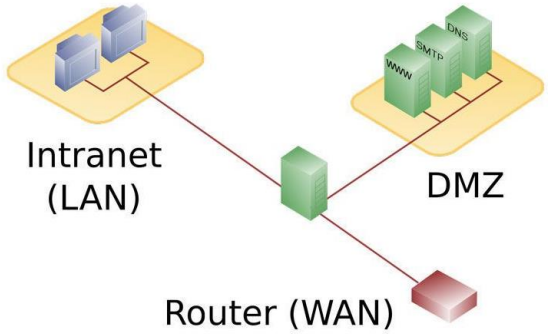
A1	Was ist eine Firewall?
A2	Weshalb, wozu und wann sollten Sie eine Firewall einsetzen?

9.1 DMZ

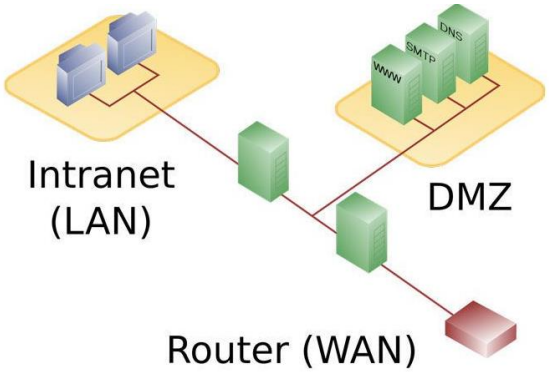
Unter der Abkürzung DMZ verstehen wir eine demilitarisierte Zone. Dies bezeichnet ein Netzwerk, wessen Serverzugriffe sicherheitstechnisch kontrolliert werden.

A1	Recherchieren Sie im Internet und informieren Sie sich über verschiedene DMZ Umsetzungen. Wie werden diese bezeichnet und was macht sie aus?
A2	Nachfolgend sehen Sie zwei mögliche Umsetzungen einer DMZ. Um welche DMZ Umsetzungen aus der vorherigen Aufgabe handelt es sich dabei? Begründen Sie Ihre Antwort!

Variante 1:



Variante 2:



Quelle: https://cdn1.vogel.de/unsafe/fit-in/1000x0/images.vogel.de/vogelonline/bdb/1341200/1341253/original.jpg

9.2 Umsetzung

Jetzt geht es um die praktische Umsetzung, wo Sie eine virtuelle Netzwerkinfrastruktur aufbauen werden. D.h. Sie werden mit Hyper-V mehrere virtuelle Maschinen aufsetzen. U.a. auch eine OPN Sense Firewall und diese entsprechend konfigurieren.

A1	Erstellen Sie im Hyper-V je einen privaten, internen und externen virtuellen Switch. Ihre Aufgabe wird es im Anschluss sein, dass Sie den privaten als LAN Segment, den internen als DMZ Segment und den externen als WAN Segment nutzen werden.
A2	Setzen Sie nun die virtuelle Firewall auf. Verwenden Sie dazu die Software OPN Sense Firewall. Die VM soll 2GB RAM, eine 10GB Festplatte und Generation 2 sein.  **WICHTIG** Fügen Sie als erstes den privaten virtuellen Switch hinzu und als zweites den externen virtuellen Switch.
A3	Prüfen Sie, dass die drei virtuellen Switches bei der Firewall auch den gewünschten Netzen entsprechen. Diese sind: External Switch ⇔ WAN Internal Switch ⇔ DMZ Private Switch ⇔ LAN  **WICHTIG** Sollte dies nicht korrekt sein, müssen Sie die Firewall erneut aufsetzen.
A4	Setzen Sie eine neue Windows Client VM auf, welche vom Hyper-V den private Switch verwendet und konfigurieren Sie diese.
A5	Können Sie mit dem Windows Client auf das Internet zugreifen? Konfigurieren Sie Ihre Windows Client VM und die Firewall so, dass Sie mit der VM ins Internet kommen.
A6	Setzen Sie eine neue Windows Server VM mit IIS auf, welche vom Hyper-V den internen Switch verwendet und konfigurieren Sie diese. Erstellen Sie auf dem IIS zwei verschiedene Webseiten.
A7	Erreichen Sie von Ihrer Windows Client VM die beiden Webseiten? Passen Sie gegebenenfalls die Regeln entsprechend an.
A8	Setzen Sie im LAN einen virtuellen Logserver basierend auf Ubuntu auf.
A9	Richten Sie die virtuellen Systeme so ein, dass sowohl der Webserver wie auch die Firewall ihre Logmeldungen an den Logserver meldet. Was können Sie alles einrichten/konfigurieren?
A10	Lösen Sie auf dem Webserver wie auch auf der Firewall unterschiedliche Ereignisse aus und analysieren Sie diese auf dem Logserver.
Z1	Richten Sie im LAN einen zusätzlichen virtuellen Server ein, auf diesem installieren Sie die Testversion von PRTG.
Z2	Richten Sie PRTG so ein, dass Sie damit Ihr komplettes Netz überwachen können.
A11	Erstellen Sie eine Präsentation von Ihrer Umsetzung und halten Sie sich bereit diese mit praktischen Elementen im Plenum zu präsentieren.