Mathias Gut | Markus Kammermann

CompTIA Security+

IT-Sicherheit verständlich erläutert

Die umfassende Prüfungsvorbereitung
zur CompTIA-Prüfung SY0-701

5. Auflage

mitp

Inhaltsverzeichnis

Kapitel 1

Laras Welt

Guten Tag, ich bin Lara aus Neustadt. Ich arbeite bei der lokalen Agentur der Nixsicura-Versicherungen und möchte euch einen Einblick in meinen beruflichen Alltag und den Umgang mit Informatik und Sicherheit geben.

Morgens bin ich jeweils die Erste, die anfängt, also schließe ich die Agentur und alle Büros auf und schalte über meine App die Kaffeemaschine ein. Anschließend gehe ich an meinen Computer und starte diesen, damit ich Zugriff auf die Daten und das Internet habe. Am Morgen genieße ich die Ruhe, da kann ich alle Mails lesen und noch ein wenig im Internet surfen und Videos schauen, was auf der Welt Interessantes geschieht. Allerdings muss ich in letzter Zeit oft darüber nachdenken, ob eine bestimmte Mail jetzt wirklich von einem Kunden oder einem Vertragspartner kommt oder nicht. Dann klicke ich zur Sicherheit jeweils auf den Anhang, dort steht ja, was ich wissen muss. Dabei hat mein Antivirenprogramm jetzt zweimal einen solchen Anhang gelöscht, dabei ich wollte doch nur nachsehen, was drin steht. Das fand ich dann doch unfair, zwei Mails waren doch sogar Bewerbungen für die neue Kundenberaterin, dass muss ich doch lesen können!

So gegen acht Uhr kommen dann die beiden Kollegen und die Chefin, und der Arbeitstag beginnt: Kunden bedienen, Links mit den eingegangenen Verträgen anklicken und öffnen, Verträge zur Unterschrift weiterleiten, Policen in der Cloud am richtigen Ort ablegen oder auch mal Reklamationen bearbeiten – was alles so anfällt in einer Versicherungsagentur. Die Daten sind für mich zum Glück alle zugänglich, so kann ich auch der Chefin mal bei einem Vertrag unter die Arme greifen oder Arbeiten meiner Kollegen ordnen und korrekt ablegen, die gerne alles einfach irgendwo speichern. Zur Sicherheit haben wir auch alle unsere Kennwörter auf einer Liste notiert, dann können wir einander problemlos helfen.

Seit Kurzem kann ich für die Ausarbeitung von Texten auch das Programm Brainfree nutzen. Dieses arbeitet mit künstlicher Intelligenz und hilft mir sehr. So kann ich einen ausführlichen Schadensbericht mit allen Daten einfach hochladen und dem Programm sagen, es soll mir eine Zusammenfassung schreiben. Mit ein paar Kundenangaben dazu kann es mir sogar ein Antwortschreiben vorschlagen. Und das alles gratis und direkt im Internet, ich finde das super praktisch.

Über Mittag gehen wir meist alle zusammen essen. Wir kennen da ein kleines Restaurant in der Nähe, das ist über Mittag zwar gut gefüllt, aber für uns halten sie immer einen Tisch frei. Das Büro schließen wir natürlich ab, die Systeme lassen wir laufen, damit wir nach der Pause nicht so viel Zeit verlieren, bis wir wieder arbeiten können.

Am Mittagstisch kann man schon mal was Privates bereden, aber auch aktuelle Vorgänge vom Vormittag, interessante Schadensfälle oder die neuesten Ideen unserer Kunden können wir hier ebenso besprechen. Das kann auch mal laut werden, aber meistens ist es einfach interessant – der Mittag ist immer schnell vorbei.

Am Nachmittag geht's wieder zurück in die Agentur. Während die beiden Kollegen dann öfter draußen bei den Kunden sind, bleibe ich in der Agentur für die Administration zuständig und erledige Telefonate oder bediene Kunden, die sich bei mir an den Tisch setzen, um mit mir ihre Sorgen oder Anliegen zu besprechen. Erst letztlich hat mich ein potenzieller Kunde sehr genau über die Vorgänge in unserer Agentur ausgefragt, da konnte ich mal zeigen, was ich alles weiß. Ein anderer stellte sich via Teams-Telefon als Regional-Finanzverantwortlicher vor und bat mich, unseren Werbeetat-Anteil an ihn sofort zu überweisen, was mir zwar komisch vorkam, aber ich möchte ja freundlich sein und habe so viele Auskünfte erteilt, wie ich konnte. So gegen 17 Uhr verlasse ich dann das Büro – abschließen tut in der Regel die Chefin, da sie meistens länger bleibt.

So weit ist eigentlich alles wie immer, wir sind organisiert, und ich bin auf meiner Stelle zufrieden. Nur nächste Woche, da müssen wir die Agentur für einen Tag schließen, weil unsere Zentrale uns alle in so eine Awareness-Schulung schicken will. Ich weiß zwar nicht, wozu das gut sein soll, bei uns ist ja noch nie etwas passiert – aber wenn es angeordnet ist, gehen wir hin und sehen, was wird. Vielleicht lässt sich ja noch etwas lernen.

1.1 Das Ziel dieses Buches

Laras Welt ist in Ordnung. Und für viele andere ist sie das auch, selbst wenn sie sich keine großen Gedanken über die Informatik machen, da sie diese als Instrument für ihre Arbeit nutzen und nicht als zentrales Thema um seinetwillen betrachten.

Oder denken Sie an IT, wenn Sie von einer Öl-Pipeline lesen? Und doch hat im Mai 2021 ein ebensolcher Angriff auf die IT-Systeme der größten amerikanischen Versorgungslinie dafür gesorgt, dass die Versorgungslinie selbst aus Sicherheitsgründen für mehrere Tage abgeschaltet werden musste. Und dies, obwohl durch diese Leitung mehr als 40 % der gesamten an der Ostküste verbrauchten Kraftstoffe laufen.

Oder denken Sie zuerst an IT, wenn Ihre Zeitung am Morgen nicht erscheint? So geschehen in Deutschland, als im April 2021 nach einem Hackerangriff zahlreiche Zeitung und Online-Portale der Madsack-Mediengruppe nicht mehr erreichbar waren oder Zeitungsteile über Tage nur in reduziertem Umfang produziert werden konnten.

Die Liste solcher und anderer Angriffe auf Unternehmen lässt sich mittlerweile täglich erweitern. Und die Folgen sind für die Unternehmen oft so gravierend, dass darüber nicht in den IT-Foren oder Security-Boards, sondern in der Tagesschau oder den Zeitungen berichtet wird. Die Angriffe zeigen überdies, wie eng die Verzahnung der eigentlichen Wertschöpfung von Unternehmen mit der Informatik und ihren Systemen mittlerweile ist – und wie manche »Laras aus Neustadt« immer noch auf unbekannte Mails klicken, sich an Telefonen ausfragen lassen oder Systeme unbeachtet laufen lassen.

Die Welt wird wegen eines neuen Buches nicht sicherer, doch mit wachsendem Bewusstsein für die Gefahren, denen unsere Daten und Systeme heute ausgesetzt sind, lässt sich künftig wenigstens ein Teil solcher Angriffe erschweren oder verhindern.

Unser Buch soll dazu die notwendigen Anleitungen, Hilfestellungen, Erklärungen und praktischen Hinweise liefern, damit Ihnen das auch gelingen kann, – und Sie darüber hinaus auf die entsprechende Zertifizierung Ihrer Fähigkeiten als CompTIA-Security+-Techniker/-in gründlich vorbereiten.

Die folgenden Kapitel dieses Buches möchten Ihnen dazu das notwendige Wissen vermitteln und Ihnen eine Orientierung anbieten, damit Sie sich anschließend in den verschiedenen Themenbereichen der Netzwerk- und Systemsicherheit auskennen. So sind Sie auch in der Lage, sich von verschiedenen Seiten her mit der Thematik auseinanderzusetzen: von den Modellen wie IT-Grundschutz, ISO 27000 über die Bedrohungslage bis hin zur Implementation von Maßnahmen oder eines ganzen Security-Managementsystems!

Die Inhalte dieses Buches und eventuell auch ein dazugehöriges Seminar helfen Ihnen bei dem Verständnis der technischen Begriffe, der Funktionsweise von Sicherheitsmaßnahmen und den aktuellen Bedrohungen und einem praxistauglichen Vorgehen, um die Prüfung CompTIA Security+ bestehen zu können.

1.2 Die CompTIA Security+-Zertifizierung

CompTIA ist ein weltweiter Verband der Informationstechnologieindustrie. CompTIA hat Mitglieder in mehr als 100 Ländern und liefert Technologiestandards in den Bereichen internetfähige Dienstleistungen, E-Commerce, herstellerunabhängige Zertifizierung, Kundenzufriedenheit, Public Policy sowie Ausbildung. Die Arbeit von CompTIA beruht auf einem kooperierenden Mitgliedsmodell – das

heißt, Hersteller, Dienstleister und Beschäftigte der IT-Industrie arbeiten bei der Formulierung und Umsetzung konkreter Ziele zusammen.

Insbesondere im Bereich der IT-Zertifizierung hat sich CompTIA weltweit einen anerkannten Ruf erworben und ist heute der größte herstellerunabhängige Anbieter von Zertifizierungen im Bereich der Informationstechnologie. Die Basis für die anerkannte Güte der CompTIA-Zertifikate ist nicht zuletzt deren gemeinschaftliche Entwicklung durch IT-Fachkräfte und Mitgliedsunternehmen. Da ein großes Problem der IT-Branche der Wildwuchs zahlreicher Fort- und Weiterbildungsmaßnahmen ist, bietet CompTIA insbesondere im Rahmen der technischen Grundausbildung hochwertige Zertifikate an, die Privatpersonen wie Unternehmen die Orientierung auf dem unübersichtlichen Fortbildungsmarkt erleichtern sollen.

Das erklärte Ziel von CompTIA ist die Etablierung von technischen und fachlichen, aber auch ethischen und professionellen Qualitätsstandards in der IT-Industrie. Indem Unternehmen wie Cisco, Hewlett-Packard, IBM, Intel, Microsoft und Ricoh die Entwicklung der Zertifikate von CompTIA finanziell und mit ihrem Know-how unterstützen, gewinnen sie gleichzeitig Anhaltspunkte über die Fachkompetenz und ein sicheres Anforderungsprofil für die Auswahl von Mitarbeitenden.

Weltweit haben mehr als zwei Millionen Menschen CompTIA-Zertifikate in Systemtechnik, Netzwerktechnologie, Serverbetreuung und anderen Gebieten erworben.

Die CompTIA Security+-Zertifizierung wendet sich an Techniker und Technikerinnen mit eigener Berufserfahrung im Informatikbereich und bescheinigt Absolventen eine breite Kenntnis auf dem Gebiet der Sicherheitstechnologie. Das bestandene Examen bedeutet, dass Geprüfte über ausreichend Wissen verfügen, um die Bedrohungslage zu verstehen und eine Reihe von Maßnahmen zu konfigurieren bzw. in Betrieb zu nehmen. Im Rahmen der Zertifizierung werden zahlreiche herstellerunabhängige Technologien behandelt. Die CompTIA Security+-Prüfung eignet sich sehr gut als Vorbereitung auf die IT-Zertifikate diverser, im Security-Sektor aktiver Hersteller.

Damit die Zertifizierung am Markt erfolgreich bleibt, wird die Prüfung durch die CompTIA regelmäßig aktualisiert und an die aktuellen Anforderungen angepasst, und so liegt mittlerweile die 701er Version von CompTIA Security+ vor. Die Inhalte der Zertifizierung werden anschließend in Lernzieldokumenten auf der Website von CompTIA unter `http://www.comptia.org` veröffentlicht (sogenannte »Exam Objectives«).

Die CompTIA Security+-Zertifizierung teilt sich in mehrere Fachgebiete, im CompTIA-Sprachgebrauch »Domains« genannt. In der aktuellen Fassung der Prüfung (SY0-701) lauten diese Themen auf Englisch wie folgt:

Domain 1 General Security Concepts (Generelle Sicherheitskonzepte)

Domain 2 Threats, Vulnerabilities and Mitigation (Bedrohungen, Schwachstellen und Abwehrmaßnahmen)

Domain 3 Security Architecture (Sicherheitsarchitektur)

Domain 4 Security Operations (Sicherer Betrieb)

Domain 5 Security Program Management and Oversight (Verwaltung und Überwachung von Sicherheitsprogrammen)

Entsprechend erhalten Sie in diesem Handbuch zur Sicherheit alle genannten Themen und ihre Zusammenhänge ausführlich erklärt und erlernen so zugleich das für die Zertifizierung notwendige Wissen. Im Zentrum steht dabei weniger die Auflistung aller möglichen und unmöglichen Abkürzungen aus diesem Bereich, sondern die Schaffung des Verständnisses für die Thematik Sicherheit. Für die Abkürzungen finden Sie zudem ein Abkürzungsverzeichnis im Anhang dieses Buches, ebenso wie eine Zuordnung der einzelnen Lernziele zu den Inhalten des Buches.

1.3 Das Weiterbildungsprogramm von CompTIA

Halten Sie Ihre Zertifizierung mit dem Weiterbildungsprogramm (CE) von CompTIA auf dem neuesten Stand. Es ist als kontinuierliche Bestätigung Ihrer Expertise und als Werkzeug zur Erweiterung Ihres Kompetenzspektrums konzipiert.

Durch die Teilnahme am Weiterbildungsprogramm von CompTIA bleiben Sie mit neuen und sich entwickelnden Technologien auf dem Laufenden und können Ihre einmal erworbene Prüfung rezertifizieren.

Ihre CompTIA-Security+-Zertifizierung ist ab dem Tag Ihrer Prüfung drei Jahre lang gültig. Das CE-Programm ermöglicht es Ihnen, Ihre Zertifizierung in dreijährigen Abständen durch Aktivitäten und Schulungen zu verlängern, die sich auf den Inhalt Ihrer Zertifizierung beziehen. Wie Security+ selbst verfügt auch CompTIA Security+ CE über einen weltweit anerkannten ISO/ANSI-Akkreditierungsstatus.

Sie können an unterschiedlichen Aktivitäten und Schulungsprogrammen teilnehmen, darunter auch an höherwertigen Zertifizierungen, um Ihre CompTIA-Security+-Zertifizierung zu erneuern. Schließen Sie CertMaster CE ab, einen Online-CE-Kurs im eigenen Tempo, oder sammeln Sie in drei Jahren mindestens 30 Continuing Education Units (CEUs), laden Sie diese auf Ihr Zertifizierungskonto hoch, und Network+ erneuert sich automatisch.

Hinweis

Wenn Sie den an dieser Stelle von CompTIA zur Verfügung gestellten Code [redacted] nutzen, so erhalten Sie beim Kauf eines CompTIA-Prüfungs-Vouchers auf der Webseite von CompTIA 10 % Rabatt.

1.4 Voraussetzungen für CompTIA Security+

Gemäß der Website von CompTIA (`http://www.comptia.org`) sind die empfohlenen Voraussetzungen für das Bestehen der Security-Prüfung die CompTIA Network+-Zertifizierung sowie zwei Jahre Erfahrung im Netzwerkbereich mit Schwerpunkt Sicherheit oder einer Systemadministratorenrolle.

Diesen Empfehlungen stimmen die Autoren natürlich zu. Dieses Buch kann Ihnen nicht die praktische Erfahrung vermitteln, die im Bereich Netzwerktechnik nötig ist, um erfolgreich zu sein. Wenn Sie sich also auf die Zertifizierung vorbereiten möchten, lesen Sie dieses Buch, aber installieren Sie auch selbst ein Netzwerk, befassen Sie sich regelmäßig mit Sicherheitsthemen, gehen Sie in ein Training oder bauen Sie mit Kollegen eine Umgebung auf, die dafür geeignet ist, und üben Sie sich praktisch in der Erkennung von Bedrohungen, der Anwendung von Sicherheitsmaßnahmen und -konzepten.

Für weitere Informationen begeben Sie sich bitte auf die Website von CompTIA unter `http://www.comptia.org/de`. Details zur Prüfung finden Sie zudem in Kapitel 21, »Die CompTIA Security+-Prüfung«.

1.5 Persönliches

Wer sich zum ersten Mal mit der Thematik Informatiksicherheit befasst, wird vor allem eins feststellen: Es wimmelt nur so von Fremdwörtern und Fachbegriffen. Von Anti-Spam über Phishing bis zum Zombie ist alles vertreten, was das Alphabet zu bieten hat.

Als Autoren staunen wir manchmal selbst über die Vielfalt an Kreationen, die hier geschaffen werden – auch wir mussten nachdenken, als wir zum ersten Mal über »Whaling« gelesen haben ... und längst nicht alle Begriffe verfügen über den gleichen Tiefsinn oder fachlichen Rückhalt.

Ein Buch zur Informatiksicherheit zu verfassen, ist daher eine Gratwanderung zwischen der notwendigen Vermittlung von Fachwissen und der Zurückhaltung gegen ein Überborden von Pseudofachbegriffen und (vorwiegend) Anglizismen, die mehr vorgeben, als sie wirklich bedeuten.

Wir haben uns daher beim Schreiben bemüht, Ihnen einen Überblick zu ermöglichen, sich mit den zentralen Themen vertraut zu machen und vor allem die Thematik zu verstehen, aber nicht schlicht Begriffe auswendig zu lernen – obwohl sich das prüfungstechnisch nicht ganz vermeiden lässt.

Es ist unsere feste Hoffnung, dass wir Sie mit diesem Buch für die Thematik der Informationssicherheit über die reine Prüfung hinaus sensibilisieren können, Ihnen Hilfen an die Hand geben und Sie ausrüsten für einen sinnvollen und sicheren Umgang mit Informationen und Informatikmitteln in Ihrem Umfeld.

Zu den Autoren selbst:

Mathias Gut, Master of Advanced Studies ZFH in Business Analysis und Dipl. Informatiker, ist Information- und Cyber-Security-Experte. Er ist in verschiedenen Bereichen von Sicherheitsfragen ausgebildet und zertifiziert, unter anderem als zertifizierter OSSTMM Professional Security Tester (OPST), zertifizierter ICO ISMS Auditor nach ISO/IEC 27001:2022, CompTIA Advanced Security Practitioner (CASP), CompTIA Security+, CompTIA Network+, CompTIA Linux+ und hat zusätzlich ein abgeschlossenes Zertifikat CAS Information Security & Risk Management der Fachhochschule Nordwestschweiz. Er arbeitet täglich mit Fragen der Cybersicherheit und unterrichtet zudem als Dozent im Bereich der Informationstechnik mit Schwerpunkt Cyber-Sicherheit in der höheren beruflichen Bildung. Als impulsgebender Entwickler und Mitdozent des von der HWZ verliehenen CAS Cyber Security Expert übernimmt er eine aktive Rolle in der Weiterbildungslandschaft. In seiner Freizeit setzt er sich für quelloffene Software und freie Analysemethoden ein, forscht zu Themen des Living-off-the-Land Hackings und gibt Fachreferate dazu.

Markus Kammermann, ursprünglich Theologe, später weitere Berufsausbildungen zum IT-Projektleiter und Ausbilder, SCRUM Master, CompTIA Security+ und weitere Zertifizierungen, ist Autor mehrerer Fachbücher aus der CompTIA-Zertifizierungsreihe bei mitp. Allen voran das bereits in 9. Auflage erschienenen Grundlagenwerks »CompTIA Network+« sowie das in 6. Auflage verlegten Studienwerks »CompTIA A+«. Er arbeitet seit vielen Jahren als technischer Berater, Dozent und Referent in verschiedenen Ländern und ist in seiner Seele ein »Erklärer«, der nach wie vor selbst IT-Infrastruktur konzipiert, vernetzt und installiert und somit die Sicherheit in der IT tagtäglich mit seinen Kunden erlebt, auch und gerade, wenn sie nicht funktioniert. Als Dozent in der höheren beruflichen Bildung und Autor ist es ihm wichtig, nicht nur Sachverhalte darzulegen, sondern sie verständlich zu machen, denn Lernen lebt nicht vom Hören, sondern vom Verstehen und Befähigt werden.

Wir danken Herrn Rechtsanwalt Christian Mitscherlich (Partner), Herrn Rechtsanwalt Fokko Oldewurtel (Senior Associate) und Herrn Andreas Schäfer (Senior Associate) von der Kanzlei Domenig & Partner Rechtsanwälte AG für ihren wert-

vollen Beitrag zu den Themen Datenschutz, Cybercrime und KI-Recht. Ihre Kanzlei Domenig & Partner Rechtsanwälte AG aus Bern besteht aus führenden Datenschutzexperten der Schweiz, die an der Redaktion des neuen schweizerischen Datenschutzgesetzes mitgewirkt haben. Private Unternehmen und die öffentliche Hand zählen bei der Bewältigung ihrer datenschutzrechtlichen Herausforderungen auf die Hilfe des Datenschutzrechtsteams der Domenig & Partner Rechtsanwälte AG.

Anlässlich der anwaltlichen Beratung beschäftigen sich die Autoren täglich mit der Umsetzung von Vorgaben der DSGVO und des neuen schweizerischen Datenschutzgesetzes. Diese umfangreiche Praxiserfahrung ließen die Autoren bei der Redaktion des neuen Kapitels Kapitel 4, »Rechtliche Grundlagen«, der fünften Auflage dieser Publikation einfließen.

Bedanken möchten wir uns an der Stelle auch bei Markus a Campo, der an der ersten Auflage aktiv mitgearbeitet und damit etliche Vorarbeit vor allem zur 2. Auflage beigetragen hat. Er arbeitet als Berater, Autor und Schulungsreferent mit dem Schwerpunkt IT-Sicherheit. Er ist von der IHK Aachen öffentlich bestellter und vereidigter Experte im Bereich IT-Sicherheit.

Bedanken möchten wir uns an dieser Stelle zudem ausdrücklich bei den Herstellern und ihren Kommunikationsabteilungen, die uns mit Bildmaterial und Unterlagen unterstützt haben.

Ebenso möchten wir uns an dieser Stelle beim mitp-Verlag bedanken und persönlich bei Katja Völpel – ja, wir haben wieder einen Titel zusammen publiziert, und das ist erfreulich.

Und da dies heute ein aktuelles Thema ist: Dieses Buch wurde auch in der fünften Auflage nicht mit KI-basierten Tools erstellt oder revidiert, und wir haben die KI auch nicht um ihre Meinung zu unserem Buch befragt.

Wir wünschen Ihnen viele spannende Stunden, ob in einem E-Book am Tablet bzw. Computer oder mit einem gedruckten Exemplar, was übrigens, so als Randnotiz, immer noch mehr als 90 % aller Leser und Leserinnen vorziehen, und nein, diese Zahl stammt nicht von 2015 aus der ersten Auflage …

Kapitel 2

Sind Sie bereit für CompTIA Security+?

Bevor Sie sich an die eigentlichen Themen von CompTIA Security+ heranwagen, haben Sie an dieser Stelle die Gelegenheit, die Voraussetzungen für diese Zertifizierung in einem kleinen Test an sich selbst zu überprüfen.

Sie finden daher im Folgenden 25 Fragen, die sich, basierend auf den von CompTIA definierten Voraussetzungen, vorwiegend mit Netzwerkfragen befassen und Ihnen die Einschätzung erlauben sollen, ob Sie das für die folgenden Themen benötigte Verständnis und Fachwissen mitbringen.

Frage 1

Sie verkaufen Ihrem Kunden eine Komponente mit der Aufschrift »IEEE 802.11ax«. Worum handelt es sich technisch gesehen bei diesem Produkt?

A) VLAN-Technologie
B) USB-3.0-Anschluss
C) USB-1.n-Anschluss
D) WLAN-Technologie
E) FireWire-Anschluss
F) FDDI-Anschluss

Frage 2

Welches ist die maximale Segmentlänge eines Gigabit-Ethernet-Segments, wenn Sie dieses mit 1000BASE-LX verkabeln?

A) 7500 Meter
B) 5500 Meter
C) 550 Meter
D) 250 Meter
E) 100 Meter

Frage 3

In einem Unternehmen sollen sich dessen Gäste mit dem Internet verbinden können, ohne dass sie irgendeinen Zugriff auf das Firmennetzwerk erhalten. Alle Verbindungen müssen über den gleichen Switch gemanagt werden können. Was werden Sie unternehmen, um diese Anforderungen zu erfüllen?

A) RIPv2 implementieren
B) OS-PF installieren
C) Port Trunking implementieren
D) VLAN-Funktionalität implementieren

Frage 4

Bei allen folgenden Anschlüssen handelt es sich um fiberoptische Anschlüsse mit Ausnahme von:

A) BNC (British Naval Connector)
B) MT-RJ (Mechanical Transfer-Registered Jack)
C) ST (Straight Type)
D) SC (Standard Connector)

Frage 5

Ein Netzwerk gemäß 802.11n-Standard kann auf Frequenzen im folgenden Frequenzband senden:

A) 900 MHz
B) 1,9 GHz
C) 2,9 GHz
D) 5,0 GHz
E) 11,0 GHz

Frage 6

Nicht jedes Kabelmedium reagiert gleich auf elektromagnetische Störungen. Welches der folgenden Medien ist am anfälligsten für diese Störungen?

A) UTP-Kategorie 5e
B) MMF optisches Kabel
C) RG-58 Koaxial
D) F/STP-Kategorie 6a

Frage 7

Mit welchem der folgenden Geräte können Sie ein 802.3-Netzwerk mit einem 802.11-Netzwerk verbinden?

A) Modem
B) Repeater
C) PVC (Permanent Virtual Circuit)
D) Gateway
E) WAP (Wireless Access Point)

Frage 8

Welche Netzwerkschnittstelle arbeitet auf den oberen drei OSI-Layern und verbindet Netzwerke unterschiedlicher Architekturen?

A) Hub
B) Modem
C) Switch
D) Router
E) Gateway

Frage 9

Die Arbeitsstation, an der Sie gerade arbeiten, zeigt Ihnen eine Fehlermeldung. Diese besagt, dass die IP-Adresse Ihres Rechners doppelt im Netzwerk entdeckt worden ist. Nachdem Sie sich eine Ursache für dieses Problem überlegt haben, was ist Ihr nächster Schritt?

A) Einen Aktionsplan zur Lösung umsetzen
B) Zusätzliche Fakten zum Auftreten des Problems sammeln
C) Die Lösung dokumentieren
D) Den Aktionsplan testen und die Ergebnisse auswerten

Frage 10

Welcher Programmaufruf erzeugt das folgende Ergebnis auf dem Bildschirm:

Aktive Verbindungen

Proto	Lokale Adresse	Remoteadresse	Status
TCP	workstation:1135	192.168.2.68:microsoft	HERGESTELLT
TCP	workstation:3845	server05.mitp.de:HTTP	WARTEND

A) arp
B) ifconfig
C) tracert
D) netstat
E) proto /a
F) nslookup

Frage 11

Ein Benutzer meldet sich beim Administrator, dass er keinen Zugriff mehr auf das Netzwerk hat. Er kann keinen erfolgreichen *ping*-Befehl an die anderen Stationen in seinem Netz absetzen, und *ipconfig* zeigt ihm zwar eine gültige IP-Adresse an, die aber nicht das korrekte Subnetz anzeigt, in dem sich der Rechner eigentlich befindet. Welcher Ansatz beschreibt dieses Problem am ehesten richtig?

A) Der DHCP-Server hat die Kommunikationsverbindung zum passenden DNS-Server verloren.
B) Der WINS-Server ist offline.
C) Der DHCP-Server ist offline.
D) Jemand hat einen zweiten DHCP-Server aktiviert.
E) Die Netzwerkkarte ist defekt.

Frage 12

Ihr IT-Administrator hat kürzlich einen neuen DNS-Server ins Netzwerk integriert und den bisherigen DNS-Server vom Netz genommen. Der neue DNS-Server verfügt über eine neue IP-Adresse, und dieser Wechsel wurde im DHCP-Server auch eingetragen.

Dennoch können in der Folge einige Arbeitsstationen Webadressen wie z.B. `http://www.mitp.de` oder `http://www.educomp.eu` aufrufen, während andere dies nicht können. Welche Arbeitsstationen sind in der Lage, die Adresse `http://www.mitp.de` aufzurufen?

A) Jede Arbeitsstation, die seit der Umstellung den DHCP-Lease nicht erneuert hat.

B) Jede Arbeitsstation mit einer statischen IP-Adresse.

C) Jede Arbeitsstation, die mindestens über Microsoft Edge verfügt.

D) Jede Arbeitsstation, die den DHCP-Lease seit der Umstellung erneuert hat.

Frage 13

Ein Webdesigner hat den Webauftritt der Firma umgebaut und dabei so programmiert, dass ab jetzt HTTPS notwendig ist, um eine Verbindung zum Server herzustellen.

Nach dieser Umstellung ist der Webserver zwar für die Intranet-Benutzer nach wie vor zugänglich, aber vom Internet ist keine Verbindungsaufnahme mehr zu ihm möglich. Was verursacht dieses Problem am Ehesten?

A) Die Firewall des Unternehmens verweigert den Zugang auf Port 389.

B) Die Firewall des Unternehmens verweigert den Zugang auf Port 443.

C) Der Webserver des Unternehmens verweigert den Zugang auf Port 8080.

D) Der DNS-Server des Unternehmens ist deaktiviert.

Frage 14

Welches der folgenden Kommandos resultiert in der Anzeige der MAC-Adresse eines bestimmten Computers?

A) nslookup

B) ipconfig /all

C) nbtstat -r

D) netstat

Frage 15

Eine Antivirensoftware bietet dann den besten Schutz, wenn sie ... (vervollständigen Sie bitte den Satz korrekt):

A) auf den Arbeitsstationen installiert ist, die mit dem Internet verbunden sind.

B) auf den Servern installiert ist.

C) auf den Servern und allen Arbeitsstationen installiert ist.

D) auf dem Internet-Gateway installiert ist.

Frage 16

Der Netzwerkadministrator muss das Notebook eines Außendienstmitarbeiters einrichten. Dabei muss er dem Verkäufer ermöglichen, im Außeneinsatz via Internet eine sichere Verbindung zum Firmennetzwerk aufbauen zu können. Was muss der Administrator bei der Einrichtung konfigurieren?

A) Er installiert das IPX/SPX-Protokoll für sicheren Datenaustausch.

B) Er installiert eine Firewall auf dem Laptop.

C) Er richtet einen drahtlosen Zugang ein.

D) Er erstellt eine PPTP-Verbindung.

E) Er stellt sicher, dass die Antivirensoftware jederzeit auf dem neuesten Stand ist.

Frage 17

Ihr Netzwerkadministrator implementiert mehrere VLANs auf einem Switch. Welches Gerät bzw. welche Funktionalität benötigt er dabei, um den Datenverkehr zwischen den verschiedenen VLANs zu ermöglichen?

A) Nichts

B) Einen zweiten Switch

C) Einen zusätzlichen Switch pro VLAN

D) Einen Router

Frage 18

Beim Einsatz einer Routing-Tabelle wird welche der folgenden Routen am *ehesten* ausgewählt?

A) Die niedrigste administrative Distanz

B) Die höchste administrative Distanz

C) Die BGP-Route

D) Die Route mit dem höchsten Hop-Count

Frage 19

Wenn ein Windows-Netzwerk auf eine Ressource zugreift, werden die »Credentials« (Zugriffsberechtigungen) durch den Gebrauch eines _____ (setzen Sie den korrekten Begriff ein) übertragen.

A) Passworts
B) Tokens
C) Cookies
D) Keys
E) Usernames

Frage 20

Sie installieren ein neues Netzwerk und setzen dazu zwei Domaincontroller auf. Der eine hat die Adresse 192.168.25.5 und der andere die Adresse 192.168.25.140. Beide fungieren als DHCP-Server im Range 192.168.25.1 – 192.168.25.254 mit dem Subnetz 255.255.255.0. Nach der Installation treten verschiedentlich DHCP-Fehler auf. Wie können Sie diese beheben?

A) Ändern Sie das Subnetz auf 255.255.0.0, damit Sie mehr verfügbare Adressen erhalten.
B) Die Server halten die IP-Adressen zu lange im Cache Memory fest. Booten Sie die beiden Server neu, und das Problem ist behoben.
C) Teilen Sie den DHCP-IP-Bereich zwischen den beiden Servern auf, indem Sie den Bereich im DHCP-Server halbieren, sodass einer die Adressen von 192.168.25.1 bis 127 und der andere von 192.168.25.128 bis 254 vergibt.
D) Teilen Sie den DHCP-IP-Bereich zwischen den beiden Servern auf, indem Sie das Subnetz auf 255.255.255.128 ändern und den IP-Bereich halbieren, sodass einer die Adressen von 192.168.25.1 bis 127 und der andere von 192.168.25.128 bis 254 vergeben kann.

Frage 21

Sie arbeiten als Netzwerkadministrator in Ihrer Firma. Sie müssen den Bandbreitenbedarf für das Internet reduzieren. Wie können Sie dies erreichen?

A) Sie installieren einen WINS-Server.
B) Sie installieren einen Proxyserver.
C) Sie installieren einen HTTP-Dienst.
D) Sie installieren einen DHCP-Server.
E) Sie installieren einen DNS-Server.
F) Sie installieren eine Firewall.

Frage 22

Der Systemadministrator konfiguriert den MS-Exchange-Server für den Einsatz von E-Mail. Der Server muss dabei Mails an die Partnerfirma versenden können, die ihrerseits einen postfix-Server einsetzt. Welches Protokoll wird eingesetzt, um Mails zwischen diesen beiden Servern hin- und herzusenden?

A) POP3 (Post Office Protocol Version 3)
B) CSNW (Client Service for NetWare)
C) SMTP (Simple Mail Transfer Protocol)
D) TCP/IP
E) WNMG (Windows NetWare Mail Gateway)

Frage 23

Der Administrator eines Netzwerks ist zuständig für ein kleines lokales Netzwerk, in dem zehn Stationen verkabelt durch einen Switch verbunden sind. Der Switch wiederum ist an einen Router angeschlossen, der die Verbindung ins Internet sicherstellt. Eines Tages wird er von einem Benutzer um Hilfe gebeten, weil dieser nicht mehr ins Internet kommt. Alle anderen Benutzer haben aber Zugriff auf das Internet. Was muss dieser Administrator prüfen, um dieses Problem anzugehen?

A) Netzwerkkarte der betroffenen Maschine, Port des Switches, der zum Router verbunden ist
B) Netzwerkkabel von der betroffenen Maschine zum Switch, Port am Switch, bei dem dieser Rechner eingesteckt ist, Zugangskabel vom Internet zum Router
C) Netzwerkkarte der betroffenen Maschine, Netzwerkkabel von dieser Maschine zum Switch, Port am Switch, bei dem dieser Rechner eingesteckt ist
D) Netzwerkkabel der betroffenen Maschine, Netzwerkkabel aller anderen Benutzer und deren Ports am Switch, Uplink-Port zum Router

Frage 24

Ihr Unternehmen möchte für das neue Verkaufssystem eine sichere Netzwerkumgebung einrichten. Daher muss der Netzwerkverkehr dieses Systems aus Sicherheitsgründen isoliert werden. Das aktuelle Adressschema lautet 10.22.33.x /24. Welche der folgenden Methoden hilft am besten, um den Verkehr zu separieren?

A) Ein dediziertes Broadcast-Netzwerk für das neue System
B) Ein dediziertes Multicast-Netzwerk für das neue System
C) Der Wechsel der IP-Adressen in ein C-Klassenschema
D) Die Einrichtung eines eigenen Subnetzes für das neue System

Frage 25

Welches Netzwerkgerät kann regelbasiert Pakete filtern?

A) Firewall

B) Layer-2-Switch

C) Hub

D) Bridge

Die Antworten zu diesen Fragen finden Sie in Abschnitt A.1, »Antworten zu den Vorbereitungsfragen«.

Das Ziel dieses Tests ist es, mindestens 72 % der Fragen richtig zu beantworten. Erreichen Sie dieses Ziel, sind Sie gut vorbereitet auf die folgenden Kapitel. Erreichen Sie dieses Ziel nicht, empfehlen wir Ihnen, sich vorab intensiver mit Netzwerktechnik auseinanderzusetzen, zum Beispiel anhand der CompTIA Network+-Zertifizierung, zu der von Markus Kammermann ebenfalls ein deutschsprachiges Buch aus dem mitp-Verlag vorliegt: »CompTIA Network+«.

Stichwortverzeichnis

D

E