Zertifizierungsprüfung CompTIA A+ Teil 2 – Prüfungsziele

PRÜFUNGSNUMMER: TEIL 2 (220-1102)

CompTIA

Über die Prüfung

Die Bewerber werden aufgefordert, dieses Dokument zur Vorbereitung auf die Zertifizierungsprüfung CompTIA A+ Teil 2 220-1102 zu verwenden. Um die Zertifizierung CompTIA A+ zu erhalten, müssen Sie zwei Prüfungen bestehen: Teil 1 (220-1101) und Teil 2 (220-1102). Mithilfe der Zertifizierungsprüfungen CompTIA A+ Teil 1 (220-1101) und Teil 2 (220-1102) werden erfolgreichen Teilnehmern die notwendigen Kenntnisse und Fähigkeiten für Folgendes bescheinigt:

- Installation, Konfiguration und Wartung von Computer-Equipment, Mobilgeräten und Software für Endbenutzer
- Wartung von Komponenten gemäß Kundenanforderungen
- Kenntnis von Netzwerkgrundlagen und Anwendung grundlegender Cybersicherheitsverfahren für die Vermeidung von Bedrohungen
- richtige und sichere Diagnose, Behebung und Dokumentation häufig auftretender Hardware- und Softwareprobleme
- Anwendung angemessener Fehlerbehebungsmaßnahmen und Bereitstellung von Kundensupport mithilfe angemessener Kommunikationsfähigkeiten
- Kenntnis der Grundlagen von Skripterstellung, Cloud-Technologien, Virtualisierung und Bereitstellung mehrerer Betriebssysteme in Unternehmen

Diese Zertifizierung entspricht einem Kenntnisstand nach 12 Monaten Praxis im Helpdesk-Support, als Desktop-Supporttechniker oder als Kundendiensttechniker im Außendienst. Diese inhaltlichen Beispiele dienen der Verdeutlichung der Testziele und sind nicht als umfassende Auflistung aller Inhalte dieser Prüfung zu verstehen.

PRÜFUNGSAKKREDITIERUNG

Die Zertifizierungsprüfung CompTIA A+ Teil 2 (220-1102) ist vom US-Normungsinstitut ANSI für die Einhaltung der ISO-Norm 17024 akkreditiert und unterliegt somit regelmäßigen Prüfungen und Aktualisierungen der Prüfungsziele.

PRÜFUNGSENTWICKLUNG

Die CompTIA-Prüfungen entstehen aus Sachverständigen-Workshops und den Ergebnissen von branchenweiten Umfragen zu den von einem IT-Experten auf Einstiegsebene geforderten Kenntnissen und Fertigkeiten.

CompTIA-RICHTLINIE ZUR NUTZUNG GENEHMIGTER MATERIALIEN

CompTIA Certifications, LLC genehmigt, befürwortet und billigt nicht die Verwendung von Inhalten, die von nicht autorisierten Schulungs-Websites von Drittanbietern (auch als „Braindumps“ bezeichnet) bereitgestellt werden. Personen, die solche Materialien zur Vorbereitung auf eine CompTIA-Prüfung nutzen, wird die Zertifizierung entzogen, und sie werden gemäß der CompTIA-Teilnehmervereinbarung von künftigen Prüfungen suspendiert. Um die Prüfungsrichtlinien von CompTIA zur Nutzung von ungenehmigten Studienmaterialien besser bekannt zu machen, leitet CompTIA alle Zertifizierungsteilnehmer zur Zertifizierungsprüfungsrichtlinie von CompTIA um. Bitte lesen Sie alle CompTIA-Richtlinien, bevor Sie mit dem Studium zur Vorbereitung auf eine der CompTIA-Prüfungen beginnen. Die Kandidaten müssen die CompTIA-Bewerber-Vereinbarung einhalten. Wenn ein Teilnehmer eine Frage dazu hat, ob Studienmaterialien als ungenehmigt (Braindumps) angesehen werden, sollte er CompTIA unter examsecurity@comptia.org kontaktieren.

BITTE BEACHTEN

Die nachfolgend aufgeführten Beispiele in den Stichpunkten sind keine vollständigen und festen Listen. Andere Beispiele von Technologien, Prozessen oder Aufgaben, die sich auf die einzelnen Schulungsziele beziehen, können ebenfalls in die Prüfung aufgenommen werden, selbst wenn sie in diesem Dokument nicht aufgeführt sind. CompTIA überarbeitet den Inhalt der Prüfungen und aktualisiert Prüfungsfragen laufend, damit die Prüfungen auf dem neuesten Stand sind und die Sicherheit der Fragen gewahrt wird. Bei Bedarf veröffentlichen wir aktualisierte Prüfungen auf der Grundlage bestehender Prüfungsziele. Sie können sicher sein, dass alle zugehörigen Vorbereitungsmaterialien weiterhin gültig sind.

PRÜFUNGSDETAILS

Erforderliche Prüfung	A+ Teil 2 (220-1102)
Anzahl der Fragen	Maximal 90
Fragentypen	Mehrfachauswahl und simulationsbasiert
Dauer der Prüfung	90 Minuten
Empfohlene Vorerfahrung	12 Monate praktische Erfahrung als Helpdesk-Supporttechniker, Desktop-Supporttechniker oder Kundendiensttechniker im Außendienst
Für das Bestehen erforderliche Punktzahl	700 (auf einer Skala von 100 - 900)

PRÜFUNGSZIELE (DOMAINS)

In der nachfolgenden Tabelle finden Sie die prüfungsrelevanten Wissensgebiete und deren Umfang in der Prüfung.

DOMAIN		PROZENTUALER ANTEIL VON DER PRÜFUNG
1.0	Betriebssysteme	31 %
2.0	Sicherheit	25 %
3.0	Software-Fehlerbehebung	22 %
4.0	Arbeitsabläufe	22 %
Insgesamt		**100 %**

HINWEIS ZU WINDOWS 11

Versionen von Microsoft® Windows®, deren Support durch Microsoft noch nicht eingestellt wurde (einschließlich der neuesten Versionen bis Windows 11), werden als für die Zertifizierung relevant betrachtet. Somit können Prüfungsziele, bei denen keine bestimmte Version von Microsoft Windows genannt wird, auch Inhalte zu Windows 10 und Windows 11 betreffen, die für die jeweiligen Aufgabenbereiche relevant sind.

1.0 Betriebssysteme

1.1 Grundeigenschaften verschiedener Versionen von Microsoft Windows erkennen

- **Versionen von Windows 10**
  - Home
  - Pro
  - Pro for Workstations
  - Enterprise
- **Funktionsunterschiede**
  - Domänenzugriff vs. Arbeitsgruppe
  - Desktop-Stile/ Benutzeroberfläche
  - Verfügbarkeit des Remote Desktop Protocol (RDP)
  - Supporteinschränkungen für den Arbeitsspeicher (RAM)
  - BitLocker
  - gpedit.msc
- **Upgrade-Pfade**
  - In-Place Upgrade

1.2 Geeignete Microsoft-Befehlszeilentools im Rahmen eines vorgegebenen Szenarios anwenden

- **Navigation**
  - cd
  - dir
  - md
  - rmdir
  - Eingaben für die Laufwerknavigation:
    - C: oder D: oder x:
- **Befehlszeilen-Tools**
  - ipconfig
  - ping
  - hostname
  - netstat
  - nslookup
  - chkdsk
  - net user
  - net use
  - tracert
  - format
  - xcopy
  - copy
  - robocopy
  - gpupdate
  - gpresult
  - shutdown
  - sfc
  - [Name des Befehls] /?
  - diskpart
  - pathping
  - winver

1.3 Funktionen und Tools des Betriebssystems Microsoft Windows 10 im Rahmen eines vorgegebenen Szenarios anwenden

- **Taskmanager**
  - Dienste
  - Start
  - Leistung
  - Prozesse
  - Benutzer
- **Snap-in Microsoft Management Console (MMC)**
  - Ereignisanzeige (eventvwr.msc)
  - Datenträgerverwaltung (diskmgmt.msc)
  - Taskplaner (taskschd.msc)
  - Geräte-Manager (devmgmt.msc)
  - Zertifikat-Manager (certmgr.msc)
  - lokale Benutzer und Gruppen (lusrmgr.msc)
  - Leistungsüberwachung (perfmon.msc)
  - Editor für lokale Gruppenrichtlinien (gpedit.msc)
- **weitere Tools**
  - Systeminformationen (msinfo32.exe)
  - Ressourcenmonitor (resmon.exe)
  - Systemkonfiguration (msconfig.exe)
  - Datenträgerbereinigung (cleanmgr.exe)
  - Datenträgerdefragmentierung (dfrgui.exe)
  - Registrierungs-Editor (regedit.exe)

1.4 Geeignete Dienstprogramme der Microsoft-Windows-10-Systemsteuerung im Rahmen eines vorgegebenen Szenarios nutzen

- **Internet-Optionen**
- **Geräte und Drucker**
- **Programme und Funktionen**
- **Netzwerk- und Freigabecenter**
- **System**
- **Windows Defender Firewall**
- **E-Mail**
- **Ton**
- **Benutzerkonten**
- **Gerätemanager**
- **Indizierungsoptionen**
- **Verwaltungstools**
- **Datei-Explorer-Optionen**
  - versteckte Dateien anzeigen
  - Erweiterungen ausblenden
  - allgemeine Optionen
  - Optionen anzeigen
- **Energieoptionen**
  - Ruhezustand
  - Energiesparpläne
  - Energiesparmodus/anhalten
  - Standby
  - auswählen, was beim Zuklappen des Computers geschehen soll
  - Schnellstart aktivieren
  - selektives USB-Energiesparen
- **erleichterte Bedienung**

1.5 Geeignete Windows-Einstellungen im Rahmen eines vorgegebenen Szenarios verwenden

- **Zeit und Sprache**
- **Update und Sicherheit**
- **Personalisierung**
- **Apps**
- **Datenschutz**
- **System**
- **Geräte**
- **Netzwerk und Internet**
- **Gaming**
- **Konten**

1.6 Microsoft-Windows-Netzwerk im Rahmen eines vorgegebenen Szenarios auf einem Client/Desktop konfigurieren

- **Arbeitsgruppen- vs. Domäneneinrichtung**
  - freigegebene Ressourcen
  - Drucker
  - Dateiserver
  - zugeordnete Laufwerke
- **lokale Betriebssystem-Firewall-Einstellungen**
  - Anwendungseinschränkungen und -ausnahmen
  - Konfiguration
- **Konfiguration des Kundennetzwerks**
  - Internet-Protocol-(IP-) Adressierungsschema
  - Domain-Name-System-(DNS-) Einstellungen
  - Subnetzmaske
  - Gateway
  - statisch vs. dynamisch
- **Netzwerkverbindungen herstellen**
  - virtuelles privates Netzwerk (VPN)
  - drahtlos
  - verkabelt
  - Wireless wide area network (WWAN)
- **Proxy-Einstellungen**
- **öffentliches vs. privatem Netzwerk**
- **Navigation im Datei-Explorer – Netzwerkpfade**
- **getaktete Verbindungen und Beschränkungen**

1.7 Anwendungsinstallations- und -konfigurationskonzepte im Rahmen eines vorgegebenen Szenarios anwenden

- **Systemanforderungen für Anwendungen**
  - 32-Bit- vs. 64-Bit-basierte Anwendungsanforderungen
  - dedizierte vs. Integrierte Grafikkarte
  - Anforderungen an Video Random-Access Memory (VRAM)
  - RAM-Anforderungen
  - Anforderungen an zentrale Prozessoreinheit (CPU)
  - externe Hardware-Token
  - Speicherplatzanforderungen
- **Betriebssystemanforderungen für Anwendungen**
  - Anwendungskompatibilität mit Betriebssystem
  - 32-Bit- vs. 64-Bit-Betriebssystem
- **Verteilungsverfahren**
  - physische Medien vs. Downloads
  - ISO-Mount
- **weitere Einflussfaktoren auf neue Anwendungen**
  - Auswirkungen auf das Gerät
  - Auswirkungen auf das Netzwerk
  - Auswirkungen auf den Betrieb
  - Auswirkungen auf das Unternehmen

1.8 Geläufige Betriebssystemtypen und deren Zwecke erläutern

- **Workstation-Betriebssysteme**
  - Windows
  - Linux
  - macOS
  - Chrome OS
- **Betriebssysteme für Handys/ Tablets**
  - iPadOS
  - iOS
  - Android
- **verschiedene Dateisystemtypen**
  - New Technology File System (NTFS)
  - File Allocation Table 32 (FAT32)
  - Third extended filesystem (ext3)
  - Fourth extended filesystem (ext4)
  - Apple File System (APFS)
  - Extensible File Allocation Table (exFAT)
- **Hersteller-Lebenszyklusbeschränkungen**
  - End-of-life (EOL)
  - Update-Einschränkungen
- **Kompatibilitätsprobleme zwischen verschiedenen Betriebssystemen**

1.9 Betriebssystem-Installationen und -Upgrades im Rahmen eines vorgegebenen Szenarios in einer Umgebung mit mehreren Betriebssystemen durchführen

- **Bootmethoden**
  - USB
  - optische Medien
  - Netzwerk
  - Festplatten-Laufwerke/ Flash-Laufwerke
  - internetbasiert
  - externes/Hot-Swap-fähiges Laufwerk
  - interne Festplatte (Partition)
- **Installationstypen**
  - Upgrade
  - Wiederherstellungspartition
  - Neuinstallation
  - Image-Bereitstellung
  - Installation reparieren
  - Remote-Netzwerkinstallation
  - weitere Einflussfaktoren
    - Treiber von Drittanbietern
- **Partitionierung**
  - GUID [Globally Unique Identifier] Partition Table (GPT)
  - Master Boot Record (MBR)
- **Festplattenformat**
- **Upgrade-Faktoren**
  - Sicherungsdateien und Benutzervorlieben
  - Unterstützung von Anwendungen und Treibern/ Rückkompatibilität
  - Hardware-Kompatibilität
- **Funktions-Updates**
  - Produktlebenszyklus

1.10 Geläufige Funktionen und Tools von macOS/ Desktop-Betriebssystemen bestimmen

- **Installation und Deinstallation von Anwendungen**
  - Dateitypen
    - .dmg
    - .pkg
    - .app
  - App Store
  - Deinstallationsverfahren
- **Apple ID und Beschränkungen durch das Unternehmen**
- **bewährte Vorgehensweisen**
  - Backups
  - Antivirus
  - Updates/Patches
- **Systemeinstellungen**
  - Anzeigen
  - Netzwerke
  - Drucker
  - Scanner
  - Datenschutz
  - Barrierefreiheit
  - Time Machine
- **Funktionen**
  - mehrere Desktops
  - Mission Control
  - Keychain
  - Spotlight
  - iCloud
  - Gesten
  - Finder
  - Remote-Disc
  - Dock
- **Disk Utility**
- **FileVault**
- **Terminal**
- **sofort beenden**

1.11 Geläufige Funktionen und Tools von Linux-Client-/ Desktop-Betriebssystemen bestimmen

- **geläufige Befehle**
  - ls
  - pwd
  - mv
  - cp
  - rm
  - chmod
  - chown
  - su/sudo
  - apt-get
  - yum
  - ip
  - df
  - grep
  - ps
  - man
  - top
  - find
  - dig
  - cat
  - nano
- **bewährte Vorgehensweisen**
  - Backups
  - Antivirus
  - Updates/Patches
- **Werkzeuge**
  - Shell/Terminal
  - Samba

2.0 Sicherheit

2.1 Verschiedene Sicherheitsvorkehrungen und deren Zwecke zusammenfassen

- **physische Sicherheit**
  - Vorraum mit Einlasskontrolle
  - Ausweisleser
  - Videoüberwachung
  - Alarmsysteme
  - Bewegungssensoren
  - Türschlösser
  - Schlösser an Ausstattung
  - Wachleute
  - Poller
  - Zäune
- **physischer Schutz für Mitarbeiter**
  - Schlüsselanhänger
  - Smart Cards
  - Schlüssel
  - Biometrie
    - Netzhautscanner
    - Fingerabdruckscanner
    - Handflächenscanner
  - Beleuchtung
  - Magnetometer
- **lokale Sicherheit**
  - Prinzip des geringsten Privilegs
  - Zugriffskontrolllisten (ACL)
  - Multifaktor-Authentifizierung (MFA)
  - E-Mail
  - Hard Token
  - Soft Token
  - Kurzmitteilungsdienst (SMS)
  - Sprachanruf
  - Authentifikator-Anwendung
- **Mobile Device Management (MDM)**
- **Active Directory**
  - Anmeldeskript
  - Domäne
  - Gruppenrichtlinien/-Updates
  - Organisationseinheiten
  - Home-Ordner
  - Ordnerumleitung
  - Sicherheitsgruppen

2.2 Drahtlose Sicherheitsprotokolle und Authentifizierungsmethoden vergleichen und einander gegenüberstellen

- **Protokolle und Verschlüsselung**
  - WiFi Protected Access 2 (WPA2)
  - WPA3
  - Temporal Key Integrity Protocol (TKIP)
  - Advanced Encryption Standard (AES)
- **Authentifizierung**
  - Remote Authentication Dial-In User Service (RADIUS)
  - Terminal Access Controller Access-Control System (TACACS+)
  - Kerberos
  - Multifaktor

2.3 Malware im Rahmen eines vorgegebenen Szenarios mit geeigneten Tools und Methoden erkennen, entfernen und vorbeugen

- **Malware**
  - Trojaner
  - Rootkit
  - Virus
  - Spyware
  - Ransomware
  - Keylogger
  - Bootsektorvirus
  - Cryptominer
- **Tools und Methoden**
  - Wiederherstellungsmodus
  - Antivirus
  - Anti-Malware
  - Software-Firewalls
  - Anti-Phishing-Schulung
  - Aufklärung der Benutzer über geläufige Bedrohungen
  - Neuinstallation des Betriebssystems

2.4 Geläufige Social-Engineering-Angriffe, Bedrohungen und Schwachstellen erläutern

- **Social Engineering**
  - Phishing
  - Vishing
  - Shoulder Surfing
  - Whaling
  - Tailgating
  - Identitätsdiebstahl
  - Dumpster Diving
  - Evil Twin
- **Bedrohungen**
  - Distributed Denial of Service (DDoS)
  - Denial of Service (DoS)
  - Zero-Day-Angriff
  - Spoofing
  - On-Path-Angriff
  - Brute-Force-Angriff
  - Wörterbuchangriff
  - interne Bedrohung
  - Injektion von Structured Query Language (SQL)
  - Cross-Site.Skripterstellung (XSS)
- **Schwachstellen**
  - nicht konforme Systeme
  - nicht gepatchte Systeme
  - ungeschützte Systeme (ohne Antivirus/Firewall)
  - nicht mehr unterstützte Betriebssysteme
  - Bring Your Own Device (BYOD)

2.5 Grundlegende Sicherheitseinstellungen im Rahmen eines vorgegebenen Szenarios im Betriebssystem Microsoft Windows verwalten und konfigurieren

- **Defender Antivirus**
  - aktivieren/deaktivieren
  - aktualisierte Definitionen
- **Firewall**
  - aktivieren/deaktivieren
  - Anschlusssicherheit
  - Anwendungssicherheit
- **Benutzer und Gruppen**
  - lokales vs. Microsoft-Konto
  - Standardkonto
  - Administrator
  - Gastbenutzer
  - Hauptbenutzer
- **Anmeldeoptionen im Betriebssystem**
  - Benutzername und Passwort
  - Personal Identification Number (PIN)
  - Fingerabdruck
  - Gesichtserkennung
  - einmalige Anmeldung (SSO)
- **NTFS vs. Freigabeberechtigungen**
  - Datei- und Ordnerattribute
  - Vererbung
- **als Administrator bzw. als Standardbenutzer ausführen**
  - User Account Control (UAC)
- **BitLocker**
- **BitLocker To Go**
- **Encrypting File System (EFS)**

2.6 Eine Workstation im Rahmen eines vorgegebenen Szenarios so konfigurieren, dass sie bewährte Vorgehensweisen im Bereich Sicherheit erfüllt

- **Verschlüsselung gespeicherter Daten**
- **bewährte Vorgehensweisen für Passwörter**
  - Komplexitätsanforderungen
    - Länge
    - Typen zu verwendender Zeichen
  - Ablaufanforderungen
  - Passwörter für BIOS (Basis-Eingabe-/Ausgabesystem) / Unified Extensible Firmware Interface (UEFI) (Einheitliche erweiterbare Firmware-Schnittstelle)
- **bewährte Vorgehensweisen für Endbenutzer**
  - Bildschirmsperre verwenden
  - bei Nichtverwendung abmelden
  - wichtige Hardware (wie Laptops) sichern/schützen
  - personenbezogene Daten (PII) und Passwörter schützen
- **Kontoführung**
  - Benutzergenehmigungen beschränken
  - Anmeldezeiten beschränken
  - Gastkonto deaktivieren
  - Sperrung nach fehlgeschlagenen Versuchen aktivieren
  - Timeout/Bildschirmsperre verwenden
- **Standard-Admin-Benutzerkonto/-Passwort ändern**
- **AutoRun deaktivieren**
- **AutoPlay deaktivieren**

2.7 Geläufige Verfahren für den Schutz von Mobilgeräten und eingebetteten Geräten erläutern

- **Bildschirmsperren**
  - Gesichtserkennung
  - PIN-Codes
  - Fingerabdruck
  - Muster
  - Streichen
- **Remote-Reinitialisierung**
- **Locator-Anwendungen**
- **Betriebssystem-Updates**
- **Geräteverschlüsselung**
- **Remote-Backup-Anwendungen**
- **Einschränkungen bei fehlgeschlagenen Anmeldeversuchen**
- **Antivirus/Anti-Malware**
- **Firewalls**
- **Richtlinien und Verfahren**
  - Privatgerät vs. firmeneigenes Handy
  - Sicherheitsanforderungen an Profile
- **Internet der Dinge (IoT)**

2.8 Geläufige Datenvernichtungs- und Entsorgungsmethoden im Rahmen eines vorgegebenen Szenarios anwenden

- **physische Zerstörung**
  - bohren
  - schreddern
  - entmagnetisieren
  - verbrennen
- **bewährte Vorgehensweisen für Recycling oder Wiederverwendung**
  - Löschen/unwiederbringliches Löschen
  - Low-Level-Formatierung
  - Standardformatierung
- **Outsourcing-Konzepte**
  - Drittanbieter
  - Zertifizierung der Zerstörung/des Recyclings

2.9 Geeignete Sicherheitseinstellungen im Rahmen eines vorgegebenen Szenarios für verkabelte und drahtlose Netzwerke für Kleinbüros konfigurieren

- **Privat-Router-Einstellungen**
  - Standardpasswörter ändern
  - IP-Filter
  - Firmware-Updates
  - Inhaltsfilterung
  - physische Platzierung/sicherer Standort
  - Reservierungen mit Dynamic Host Configuration Protocol (DHCP)
  - Static-Wide-Area-Network-(WAN-) IP
  - Universal Plug and Play (UPnP)
  - sicherheitsüberwachtes Subnetz
- **speziell für drahtlose Netzwerke**
  - Service Set Identifier (SSID) ändern
  - SSID-Übertragung deaktivieren
  - Verschlüsselungseinstellungen
  - Gastzugriff deaktivieren
  - Kanäle wechseln
- **Firewall-Einstellungen**
  - ungenutzte Anschlüsse deaktivieren
  - Portweiterleitung/-zuordnung

2.10 Browser und relevante Sicherheitseinstellungen im Rahmen eines vorgegebenen Szenarios installieren und konfigurieren

- **Browser-Download/-Installation**
  - vertrauenswürdige Quellen
    - Hashing
  - nicht vertrauenswürdige Quellen
- **Erweiterungen und Plug-ins**
  - vertrauenswürdige Quellen
  - nicht vertrauenswürdige Quellen
- **Passwortmanager**
- **Sichere Verbindungen/Sites – gültige Zertifikate**
- **Einstellungen**
  - Pop-up-Blocker
  - Browserdaten löschen
  - Cache leeren
  - Privatmodus
  - Anmeldung/Browserdatensynchronisierung
  - Ad-Blocker

3.0 Software-Fehlerbehebung

3.1 In einer bestimmten Situation geläufige Probleme mit Windows-Betriebssystemen beheben

- **häufige Symptome**
  - Blue Screen of Death (BSOD)
  - langsames Gerät
  - Probleme beim Booten
  - häufiges Abschalten
  - Dienste starten nicht
  - Anwendungen stürzen ab
  - Warnungen über wenig Speicherplatz
  - Ressourcenwarnungen für USB-Steuerung
  - Systeminstabilität
  - kein Betriebssystem gefunden
  - langsames Laden des Profils
  - Driften der Systemzeit
- **geläufige Schritte für die Fehlerbehebung**
  - Neustart
  - Dienste neu starten
  - Anwendungen deinstallieren/neu installieren/aktualisieren
  - Ressourcen hinzufügen
  - Anforderungen prüfen
  - Systemdateien prüfen
  - Windows reparieren
  - Wiederherstellung
  - Reimaging
  - Aktualisierungen zurücksetzen
  - Windows-Profile neu erstellen

3.2 Geläufige Fehler und Sicherheitsmängel im Rahmen eines vorgegebenen Szenarios an einem PC beheben

- **häufige Symptome**
  - kein Zugriff auf das Netzwerk
  - Desktop-Fehlermeldungen
  - falschpositive Fehlermeldungen des Virenschutzes
  - veränderte System- oder persönliche Dateien
    - fehlende/umbenannte Dateien
  - unerwünschte Benachrichtigungen des Betriebssystems
  - Fehler bei Betriebssystem-Updates
- **browserbezogene Symptome**
  - zufällige/häufige Pop-ups
  - Zertifikat-Warnmeldungen
  - Umleitung

3.3 Bewährte Vorgehensweisen zum Entfernen von Malware im Rahmen eines vorgegebenen Szenarios anwenden

1. **Malware-Symptome prüfen und bestätigen**
2. **Infizierte Systeme unter Quarantäne stellen**
3. **Systemwiederherstellung in Windows deaktivieren**
4. **Infiziertes System wiederherstellen**
   a. Anti-Malware-Software aktualisieren
   b. Scan- und Beseitigungstechniken (z. B. abgesicherter Modus, Preinstallation Environment) anwenden
5. **Scans planen und Updates ausführen**
6. **Systemwiederherstellung in Windows aktivieren und Wiederherstellungspunkte schaffen**
7. **Endnutzer aufklären**

3.4 Geläufige Probleme mit Mobilgeräte-Betriebssystemen und Anwendungen im Rahmen eines vorgegebenen Szenarios beheben

- **häufige Symptome**
  - Anwendung startet nicht
  - Anwendung schließt sich nicht/stürzt ab
  - Anwendung kann nicht aktualisiert werden
  - langsames Ansprechen
  - Betriebssystem kann nicht aktualisiert werden
  - Probleme mit der Akkulebensdauer
  - willkürliche Neustarts
  - Konnektivitätsprobleme
    - Bluetooth
    - WLAN
    - Nahfeldkommunikation (NFC)
    - AirDrop
  - Bildschirm dreht sich nicht automatisch

3.5 Geläufige Probleme mit der Sicherheit von Mobilgeräte-Betriebssystemen und Anwendungen im Rahmen eines vorgegebenen Szenarios beheben

- **Sicherheitsbedenken**
  - Quelle des Android Package (APK)
  - Entwicklermodus
  - Root-Zugriff/Jailbreak
  - Bootleg/bösartige Anwendung
    - Anwendungs-Spoofing
- **häufige Symptome**
  - hohes Netzwerk-Traffic-Aufkommen
  - langsames Ansprechen
  - Benachrichtigung über Erreichen des Datenlimits
  - eingeschränkte Internetverbindung
  - keine Internetverbindung
  - hohe Anzahl an Werbeanzeigen
  - gefälschte Sicherheitswarnungen
  - unerwartetes Verhalten von Anwendungen
  - Durchsickern persönlicher Dateien/Daten

4.0 Arbeitsabläufe

4.1 Bewährte Vorgehensweisen für Dokumentation und Supportsystem-Informationsmanagement im Rahmen eines vorgegebenen Szenarios anwenden

- **Ticketsysteme**
  - Benutzerdaten
  - Gerätedaten
  - Problembeschreibung
  - Kategorien
  - Schweregrad
  - Eskalationsstufen
  - klar verständliche, präzise schriftliche Kommunikation
    - Problembeschreibung
    - Notizen zum Fortschritt
    - Problemlösung
- **Asset-Management**
  - Inventarlisten
  - Datenbanksystem
  - Asset-Tags und -IDs
  - Beschaffungslebenszyklus
  - Garantie und Lizenzen
  - zugewiesene Benutzer
- **Dokumenttypen**
  - Acceptable Use Policy (Richtlinien zur akzeptablen Nutzung)
  - Netzwerktopologiediagramm
  - gesetzliche Anforderungen
    - Splash Screens
  - Vorfallsberichte
  - Standardbetriebsverfahren
    - Verfahren für die individuelle Installation von Softwarepaketen
  - Checkliste für die Einrichtung neuer Benutzer
  - Checkliste für die Deaktivierung alter Endbenutzer
- **Wissensdatenbank/Artikel**

4.2 Grundlegende bewährte Vorgehensweisen für Change-Management erläutern

- **dokumentierte Geschäftsprozesse**
  - Rücknahmeplan
  - Sandbox-Tests
  - verantwortlicher Mitarbeiter
- **Change-Management**
  - Anforderungsformulare
  - Zweck der Änderung
  - Umfang der Änderung
  - Datum und Uhrzeit der Änderung
  - betroffene Systeme / Auswirkungen
  - Risikoanalyse
    - Risikostufe
  - Genehmigung des Change Board
  - Endbenutzerakzeptanz

4.3 Methoden zur Sicherung und Wiederherstellung einer Workstation im Rahmen eines vorgegebenen Szenarios implementieren

- **Sicherung und Wiederherstellung**
  - vollständig
  - inkrementell
  - differenziell
  - synthetisch
- **Sicherungstest**
  - Häufigkeit
- **Sicherungs-Rotationsschemata**
  - On-site vs. Off-site
  - Großvater-Vater-Sohn-Schema (GFS)
  - 3-2-1-Sicherungsregel

4.4 Geläufige Sicherheitsverfahren im Rahmen eines vorgegebenen Szenarios anwenden

- **ESD-Ableitbänder**
- **ESD-Matten**
- **Erdung der Ausstattung**
- **ordnungsgemäßer Umgang mit Strom**
- **ordnungsgemäße Handhabung und Lagerung der Komponenten**
- **Antistatikbeutel**
- **Einhaltung der behördlichen Vorschriften**
- **persönliche Sicherheit**
  - Trennen der Stromversorgung vor Reparatur eines PCs
  - Hebetechniken
  - elektrischer Brandschutz
  - Schutzbrille
  - Luftfiltermaske

4.5 Auswirkungen auf die Umwelt und lokale Umweltschutzkontrollen erläutern

- **Materialsicherheitsdatenblatt (Material Safety Data Sheet MSDS) / Dokumentation für Handhabung und Entsorgung**
  - ordnungsgemäße Entsorgung von Akkus und Batterien
  - ordnungsgemäße Entsorgung von Toner
  - ordnungsgemäße Entsorgung anderer Geräte und Anlagen
- **Bewusstsein für Temperatur, Luftfeuchtigkeit, Sorge für eine angemessene Belüftung**
  - Standort/Platzierung der Ausstattung
  - Staubentfernung
  - Druckluft/Staubsauger
- **Stromstöße, Niederspannungsereignisse und Stromausfälle**
  - Batterie-/Akku-Backup
  - Überspannungsschutz

4.6 Erläutern der Bedeutung von verbotenen Inhalten/Aktivitäten sowie von Datenschutz-, Lizenzierungs- und Richtlinienkonzepten

- **Reaktion auf Vorfälle**
  - Beweiskette
  - Management/Gesetzesvollzug je nach Bedarf informieren
  - Festplatte kopieren (Datenintegrität und Erhaltung)
  - Dokumentation des Vorfalls
- **Lizenzierung/digitale Rechteverwaltung (DRM)/ Endbenutzer-Lizenzvereinbarung (EULA)**
  - gültige Lizenzen
  - nicht abgelaufene Lizenzen
  - Lizenz für den Privatgebrauch vs. Unternehmenslizenz
  - Open-Source-Lizenz
- **gesetzlich geregelte Daten**
  - Kreditkarten-Transaktionen
  - von der Regierung bereitgestellte personenbezogene Daten
  - PII
  - Gesundheitsdaten
  - Datenspeicherungsvorgaben

4.7 Angemessene Kommunikationstechniken im Rahmen eines vorgegebenen Szenarios anwenden und Professionalität unter Beweis stellen

- **professionelles Aussehen, professionelle Kleidung**
  - für die Umgebung geeignete Kleidung auswählen
    - förmlich
    - legere Geschäftskleidung (Business Casual)
- **angemessene Sprache verwenden und Akronyme, Fach- wie umgangssprachliche Ausdrücke möglichst vermeiden**
- **positive Einstellung bewahren/ Vertrauen in ein Projekt beweisen**
- **aktiv zuhören (Notizen machen) und vermeiden, den Kunden zu unterbrechen**
- **sich kulturell aufgeschlossen zeigen**
  - Fachleute ihrem Titel gerecht (sofern vorhanden) ansprechen
- **pünktlich sein (Kunden im Falle einer Verspätung vorab informieren)**
- **Ablenkungen vermeiden**
  - private Anrufe
  - Chats / soziale Medien
  - private Unterbrechungen
- **Umgang mit schwierigen Kunden oder Situationen**
  - nicht mit Kunden streiten oder sich defensiv verhalten
  - Abweisung von Kundenanliegen vermeiden
  - neutral bleiben
  - Kundenanliegen mithilfe offener Fragen besser verstehen und den Umfang des Problems erfassen; dieses sollte zusammenfassend wiederholt werden, um zu überprüfen, ob alles richtig verstanden wurde
  - Erfahrungen dürfen keinesfalls in sozialen Medien verbreitet werden
- **Erwartungen/Zeitplan festlegen und erfüllen sowie dem Kunden den jeweiligen Stand mitteilen**
  - je nach Bedarf Reparatur-/ Austauschoptionen anbieten
  - für eine ordnungsgemäße Dokumentation der angebotenen Dienste sorgen
  - Follow-up mit dem Kunden/ Benutzer zu einem späteren Termin, um zu überprüfen, ob er mit der Dienstleistung zufrieden war
- **mit vertraulichen und personenbezogenen Daten des Kunden stets angemessen umgehen**
  - auf einem Computer, Desktop, Drucker usw.

4.8 Grundlagen der Skripterstellung erkennen

- **Skriptdateiformate**
  - .bat
  - .ps1
  - .vbs
  - .sh
  - .js
  - .py
- **Anwendungsfälle für Skripterstellung**
  - grundlegende Automatisierung
  - Neustart von Computern
  - Neuzuordnung von Netzlaufwerken
  - Installation von Anwendungen
  - automatisierte Sicherungen
  - Erfassen von Informationen/Daten
  - Start von Updates
- **andere Faktoren, die es bei der Verwendung von Skripts zu berücksichtigen gilt**
  - versehentliche Einschleusung von Malware
  - versehentliche Änderung von Systemeinstellungen
  - Browser- oder Systemabstürze aufgrund der Fehlzuweisung von Ressourcen

4.9 Fernzugriffstechnologien im Rahmen eines vorgegebenen Szenarios verwenden

- **Verfahren/Tools**
  - RDP
  - VPN
  - Virtual Network Computer (VNC)
  - Secure Shell (SSH)
  - Remote Monitoring and Management (RMM)
  - Microsoft Remote Assistance (MSRA)
  - Tools von Drittanbietern
    - Bildschirmfreigabe-Software
    - Videokonferenz-Software
    - Dateiübertragungs-Software
    - Desktopmanagement-Software
- **Sicherheitsaspekte für die verschiedenen Zugriffsmethoden**

CompTIA A+ Teil 2 (220-1102): Liste der Akronyme

Folgende Akronyme werden in der Prüfung CompTIA A+ Teil 2 (220-1102) verwendet. Teilnehmer sind aufgefordert, die komplette Liste durchzugehen und sich Arbeitskenntnisse aller aufgeführten Akronyme als Teil des umfassenden Prüfungsvorbereitungsprogramms zu erwerben.

Akronym	Definition
AAA	Authentication Authorization and Accounting (Authentifizierung, Autorisierung und Accounting)
AC	Alternating Current (Wechselstrom)
ACL	Access Control List (Zugriffskontrollliste)
ADF	Automatic Document Feeder (automatischer Dokumenteneinzug)
AES	Advanced Encryption Standard (erweiterter Verschlüsselungsstandard)
AP	Access Point (Zugangspunkt)
APFS	Apple File System (Dateisystem)
APIPA	Automatic Private Internet Protocol Addressing (automatische private Internetprotokoll-Adressierung)
APK	Android Package
ARM	Advanced RISC [Reduced Instruction Set Computer] Machine (fortgeschrittene RISC-Maschine)
ARP	Address Resolution Protocol (Adressauflösungsprotokoll)
ATA	Advanced Technology Attachment
ATM	Asynchronous Transfer Mode (asynchroner Übertragungsmodus)
ATX	Advanced Technology Extended
AUP	Acceptable Use Policy (Richtlinien zur akzeptablen Nutzung)
BIOS	Basic Input/Output System (Basis-Eingabe-/Ausgabesystem)
BSOD	Blue Screen of Death
BYOD	Bring Your Own Device
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CD	Compact Disc
CDFS	Compact Disc File System
CDMA	Code Division Multiple Access (Codemultiplexverfahren)
CERT	Computer Emergency Response Team
CIFS	Common Internet File System
CMD	Command Prompt (Befehlseingabeaufforderung)
CMOS	Complementary Metal-Oxide Semiconductor (komplementäre Metalloxid-Halbleiter)
CPU	Central Processing Unit (zentrale Prozessoreinheit)
CRL	Certificate Revocation List
DC	Direct Current (Gleichstrom)
DDoS	Distributed Denial of Service
DDR	Double Data Rate
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual Inline Memory Module
DKIM	DomainKeys Identified Mail
DMA	Direct Memory Access
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
DoS	Denial of Service (Dienstverweigerung)
DRAM	Dynamic Random-Access Memory
DRM	Digital Rights Management
DSL	Digital Subscriber Line (digitaler Teilnehmeranschluss)
DVI	Digital Visual Interface
DVI-D	Digital Visual Interface-Digital
ECC	Error Correcting Code
EFS	Encrypting File System
EMI	Electromagnetic Interference (elektromagnetische Interferenz)
EOL	End-of-Life (Endes des Produktlebenszyklus)
eSATA	External Serial Advanced Technology Attachment
ESD	Electrostatic Discharge (Elektrostatische Entladung)
EULA	End-User License Agreement (Endnutzervereinbarung)
exFAT	Extensible File Allocation Table
ext	Extended File System
FAT	File Allocation Table
FAT12	12-bit File Allocation Table
FAT16	16-bit File Allocation Table
FAT32	32-bit File Allocation Table
FSB	Front-Side Bus
FTP	File Transfer Protocol (Datenübertragungsprotokoll)
GFS	Grandfather-Father-Son (Großvater-Vater-Sohn)
GPS	Global Positioning System
GPT	GUID [Globally Unique Identifier] Partition Table
GPU	Graphics Processing Unit (Grafikprozessor)

Akronym	Definition
GSM	Global System for Mobile Communications
GUI	Graphical User Interface (Grafikschnittstelle)
GUID	Globally Unique Identifier
HAL	Hardware Abstraction Layer
HAV	Hardware-assisted Virtualization (hardwaregestützte Virtualisierung)
HCL	Hardware Compatibility List
HDCP	High-bandwidth Digital Content Protection
HDD	Hard Disk Drive
HDMI	High-Definition Multimedia Interface
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol (Hypertext-Übertragungsprotokoll)
HTTPS	Hypertext Transfer Protocol Secure (Sicheres Hypertext-Übertragungsprotokoll)
I/O	Input/Output
IaaS	Infrastructure as a Service
ICR	Intelligent Character Recognition
IDE	Integrated Drive Electronics
IDS	Intrusion Detection System (Angrifferkennungssystem)
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet Mail Access Protocol
IOPS	Input/Output Operations Per Second (I/O-Leistung pro Sekunde)
IoT	Internet of Things
IP	Internet Protocol (Internetprotokoll)
IPS	Intrusion Prevention System
IPS	In-plane Switching
IPSec	Internet Protocol Security (Internetprotokollsicherheit)
IR	Infrarot
IrDA	Infrared Data Association
IRP	Incident Response Plan (Vorfallsreaktionsplan)
ISO	International Organization for Standardization
ISP	Internet Service Provider (Internetdienstanbieter)
ITX	Information Technology eXtended
KB	Knowledge Base
KVM	Keyboard-Video-Mouse (Tastatur-Video-Maus)
LAN	Local Area Network (lokales Netzwerk)
LC	Lucent Connector
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light-emitting Diode (Leuchtdiode)
MAC	Media Access Control/ Mandatory Access Control
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MBR	Master Boot Record
MDM	Mobile Device Management
MFA	Multifactor Authentication
MFD	Multifunction Device
MFP	(Multifunktionsdrucker)
MMC	Microsoft Management Console
MOU	Memorandum of Understanding (Absichtserklärung)
MSDS	Material Safety Data Sheet (Materialsicherheitsdatenblatt)
MSRA	Microsoft Remote Assistance
MX	Mail Exchange
NAC	Network Access Control (Netzwerk-Zugangskontrolle)
NAT	Network Address Translation (Netzwerk-Adressübersetzung)
NDA	Non-disclosure Agreement (Geheimhaltungsvereinbarung)
NetBIOS	Network Basic Input Output System (vernetztes Basis-Eingabe-/Ausgabesystem)
NetBT	NetBIOS over TCP/IP [Übertragungssteuerungsprotokoll/ Internet-Protokoll]
NFC	Near-field Communication (Nahfeldkommunikation)
NFS	Network File System
NIC	Network Interface Card (Netzwerkkarte)
NTFS	New Technology File System
NVMe	Non-volatile Memory Express
OCR	Optical Character Recognition
OLED	Organic Light-emitting Diode (organische Leuchtdiode)
ONT	Optical Network Terminal (optisches Netzwerkterminal)
OS	Operating System (Betriebssystem)
PaaS	Platform-as-a-Service
PAN	Personal Area Network (Kleinstnetzwerk für die persönliche Kommunikation)
PC	Personal Computer (Einzelplatzrechner)
PCIe	Peripheral Component Interconnect Express
PCL	Printer Command Language
PE	Preinstallation Environment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PoE	Power over Ethernet
POP3	Post Office Protocol 3
POST	Power-on Self-Test (Selbsttest beim Einschalten)
PPP	Point-to-Point Protocol
PRL	Preferred Roaming List
PSU	Power Supply Unit
PXE	Preboot Execution Environment
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Independent (or Inexpensive) Disks
RAM	Random-access Memory (Arbeitsspeicher)
RDP	Remote Desktop Protocol (Fernwartungsprotokoll)
RF	Radio Frequency (Funkfrequenz)
RFI	Radio Frequency Interference (Funkstörung)
RFID	Radio Frequency Identification (Funkfrequenzidentifikation)
RJ11	Registered Jack Function 11
RJ45	Registered Jack Function 45
RMM	Remote Monitoring and Management
RTO	Recovery Time Objective (gewünschte Wiederherstellungsdauer)
SaaS	Software-as-a-Service

Akronym	Definition
SAN	Storage Area Network (Speicherbereich im Netzwerk)
SAS	Serial Attached SCSI [Small Computer System Interface]
SATA	Serial Advanced Technology Attachment
SC	Subscriber Connector (Teilnehmeranschluss)
SCADA	Supervisory Control and Data Acquisition
SCP	Secure Copy Protection (Sicherer Kopierschutz)
SCSI	Small Computer System Interface (standardisierte parallele Schnittstelle)
SDN	Software-defined Networking
SFTP	Secure File Transfer Protocol (Sicheres Datenübertragungsprotokoll)
SIM	Subscriber Identity Module
SIMM	Single Inline Memory Module
S.M.A.R.T.	Self-monitoring Analysis and Reporting Technology
SMB	Server Message Block
SMS	Short Message Service (Kurzmitteilungsdienst)
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SODIMM	Small Outline Dual Inline Memory Module
SOHO	Small Office/Home Office (Kleinbüro/Heimbüro)
SPF	Sender Policy Framework
SQL	Structured Query Language
SRAM	Static Random-access Memory
SSD	Solid-State Drive (Festkörperlaufwerk)
SSH	Secure Shell
SSID	Service Set Identifier (Netzwerkname)
SSL	Secure Sockets Layer
SSO	Single Sign-on
ST	Straight Tip
STP	Shielded Twisted Pair
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol (Übertragungssteuerungsprotokoll)
TCP/IP	Transmission Control Protocol/Internet Protocol (Übertragungssteuerungsprotokoll/ Internet-Protokoll)
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TN	Twisted Nematic
TPM	Trusted Platform Module
UAC	User Account Control
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface (vereinheitlichte erweiterte Firmware-Schnittstelle)
UNC	Universal Naming Convention (Allgemeine Namenskonvention)
UPnP	Universal Plug and Play
UPS	Uninterruptible Power Supply (Unterbrechungsfreie Stromversorgung)
USB	Universal Serial Bus
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair (nicht abgeschirmtes Kabel mit verdrillten Adernpaaren)
VA	Vertical Alignment (vertikale Ausrichtung)
VDI	Virtual Desktop Infrastructure
VGA	Video Graphics Array
VLAN	Virtual LAN [Local Area Network]
VM	Virtual Machine
VNC	Virtual Network Computer
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network (Virtuelles privates Netzwerk)
VRAM	Video Random-access Memory
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WISP	Wireless Internet Service Provider
WLAN	Wireless LAN [Local Area Network]
WMN	Wireless Mesh Network
WPA	WiFi Protected Access (Verschlüsselungsart)
WWAN	Wireless Wide Area Network
XSS	Cross-Site-Skripterstellung

CompTIA A+ Teil 2 (220-1102): Liste der empfohlenen Hard- und Software

** CompTIA hat diese Musterliste mit Hard- und Software hinzugefügt, um Kandidaten bei der Vorbereitung auf die Prüfung A+ Teil 2 (220-1102) zu unterstützen. Diese Liste kann auch für Schulungsunternehmen hilfreich sein, die eine Praxiskomponente für ihr Schulungsangebot erstellen möchten. Die Aufzählungen zu den einzelnen Themen sind Beispiellisten und nicht erschöpfend.

Ausstattung

- Apple-Tablet/-Smartphone
- Android-Tablet/-Smartphone
- Windows-Tablet/-Smartphone
- Chromebook
- Windows-Laptop/Mac-Laptop/Linux-Laptop
- Windows-Desktop/Mac-Desktop/Linux-Desktop
- Windows-Server mit Active Directory und Druckverwaltung
- Monitore
- Projektoren
- SOHO-Router/-Switch
- Access Point
- Voice-over-Internet-Protocol-(VoIP-)Telefon
- Drucker
  - Laser-/Tintenstrahldrucker
  - drahtlos
  - 3D-Drucker
  - Thermodrucker
- Überspannungsschutz
- unterbrechungsfreie Stromversorgung (UPS)
- Smart Devices (IoT-Geräte)
- Server mit Hypervisor
- Klemmleiste
- Patchfeld
- Webcams
- Lautsprecher
- Mikrofone

Ersatzteile/Hardware

- Hauptplatinen
- RAM
- Festplatten
- Netzteile
- Videokarten
- Soundkarten
- Netzwerkkarten
- drahtlose Netzwerkkarten (NIC)
- Lüfter/Kühlgeräte/Kühlkörper
- CPUs
- Stecker-/Kabelsortiment
  - USB
  - High-Definition Multimedia Interface (HDMI)
  - DisplayPort
  - Digital Visual Interface (DVI)
  - Video Graphics Array (VGA)
- Adapter
  - Bluetooth-Adapter
- Netzwerkkabel
- Netzwerkkabel/Anschlüsse ohne Stecker
- Wechselstromadapter
- optische Laufwerke
- Schrauben/Abstandsbolzen
- Gehäuse
- Wartungskit
- Mäuse/Tastaturen
- Tastatur-Video-Maus (KVM)
- Konsolenkabel
- Festkörperlaufwerk (SSD)

Werkzeuge

- Schraubendreher
- Multimeter
- Kabelschneider
- LSA-Auflegewerkzeug
- Crimpzange
- Netzteiltester
- Abisolierzange
- Standard-Technikerwerkzeugset
- ESD-Ableitband
- Wärmeleitpaste
- LAN-Tester
- WLAN-Tester
- Anschluss Serial Advanced Technology Attachment (SATA) auf USB

Software

- Betriebssysteme
  - Linux
  - Chrome OS
  - Microsoft Windows
  - macOS
  - Android
  - iOS
- Live-CD/Datenträger mit Preinstallation Environment (PE)
- Antiviren Software
- Virtualisierungssoftware
- Anti-Malware
- Treibersoftware

CompTIA