**Ü1: Fehlersuche Client-Server Applikation**

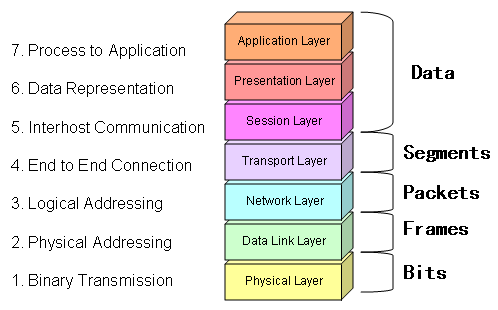
Wo liegt der "Hund" begraben?

* Info aus einer Abteilung in einer Nebenstelle, dass die Applikation XY (ein Excel mit Datenbankzugriff) sehr langsam ist und sehr oft eine Fehlermeldung kommt, dass die Daten nicht zur Verfügung stünden.
* Seitens der Abteilungsleitung wurden bereits mehrere Tickets an den Helpdesk erstellt.
* Der Helpdesk hat eine First-Level Untersuchung gemacht und keinen Fehler finden können (Remote Überwachung des Zugriffs durch Benutzer, Start aus dem Intranet der Zentrale).
* In der Known-Error Datenbank des Unternehmens ist keine weitere Ursache dokumentiert.
* Zur weiteren Abklärung wurde das Problem an den Second Level Support weitergeleitet.

1) Wie gehen sie vor, um das Problem greifbar zu machen?

**OSI Referenzmodell**

Bei komplexen Fehlern ist ein strukturiertes Vorgehen unerlässlich. Hierbei bietet sich das Vorgehen nach dem OSI-Schichtenmodell an. Beim Bottom-Up-Approach, also dem Vorgehen von unten nach oben, untersucht man ausgehend vom Physical Layer das Problem.



**Physical Layer**

Auf diesem Layer finden man Signalpegel, Stecker und Verkabelung. Typische Probleme sind falsche oder defekte Kabel, Kontaktprobleme an Steckverbindungen und falsche Geschwindigkeiten im Ethernet. Zur Fehlersuche können Kabeltester eingesetzt werden.

**Data Link Layer**

Im Data Link Layer verursachen doppelte MAC-Adressen und inkompatile Frametypen den Großteil der Probleme. Die Verbindung zum Network Layer stellt ARP her. Das entsprechende Kommando unter Linux und Windows leistet hier gute Dienste.

Auf dem Layer 2 arbeitet auch Cisco's CDP. Mit CDP kann man also sehr gut die Verbindung auf diesem Layer überprüfen.

**Network Layer**

Im Network Layer trifft man auf IP und IPX. Auch hier sind nicht eindeutige Adressen und falsche Netzmasken als Fehlerquellen sehr beliebt. Auch Routing findet in diesem Layer statt.

Zur Fehlersuche eigenen sich hier Tools wie ping und traceroute sowie die entsprechenden Kommandos auf den Routern.

**Transport Layer**

Typische Vertreter im Transport Layer sind UDP, TCP und SPX. Problemursache könnte hier eine zu kleine Windowsize im TCP sein. Als Hilfmittel zur Fehlersuche wird man zu einem Analyser greifen.

**Session Layer**

Auf dieser Schicht arbeitet beispielsweise DNS. Für eine Problemanalyse eignen sich nslookup und dig. Typisches Problem bei SMB ist die zu hohe Erwartung in die Ausnutzung der verfügbaren Bandbreite.

**Presentation Layer**

Im Presentation Layer wird die Art der Darstellung der zu übertragen Daten festgelegt. Es dreht sich also alles um Dateiformate wie ASCII, JPEG oder CSV.

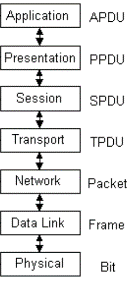
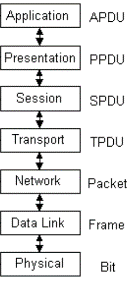
**Application Layer**

Die Applikation ist das Frontend eines Protokolls für den Anwender. So ist der Telnet-Client der Application Layer für das Protokoll Telnet.

**Strukturierte Fehlersuche**

Nicht nur bei der Fehlersuche in Netzwerken, hilft ein strukturiertes Vorgehen bei der Lösung komplexer Probleme. Zuerst sollte man sich einen Überblick über das Problem und die beteiligten Komponenten und Protokolle verschaffen. Hat man mögliche Fehlerquellen identifiziert, implementiert man eine Änderung. Und wirklich nur eine. Die Auswirkung der Änderung wird dokumentiert. Hat die Veränderung den Fehler behoben? Wenn die Maßnahme den Fehler nicht beseitigt hat, macht man die Änderung rückgängig und dokumentiert diesen Versuch. So wird der Fehler Schritt für Schritt eingegrenzt. Nie mehrere Änderungen gleichzeitig vornehmen!

2) Erstellen sie eine beispielhafte Architektur-Skizze mit den beteiligten Komponenten, die sie in Ihre Untersuchung einbeziehen würden.

Ein Bild, das Text, Himmel, grün enthält.

Automatisch generierte Beschreibung

3) Welche Maßnahmen würden Sie ergreifen, um das Problem einzugrenzen, finden und beseitigen.

**Das Problem und die Folgen eingrenzen**

Zunächst gilt es die Auswirkungen und den Umfang des Problems oder Fehlers zu klären. So kann ein beschädigtes Netzwerkkabel die Verbindung zu einem einzelnen Endgerät beeinträchtigen oder aber auch negative Folgen für ein ganzes Segment haben.

Tritt das Problem bei mehreren Nutzern auf, kann man Hardwareprobleme auf einem Endgerät oder Anwenderfehler ausschließen. Falls das Unternehmen über mehrere Standorte verfügt, gilt es zu klären, ob alle gleichermaßen betroffen sind. Damit lässt sich eingrenzen, ob das Problem auf einem der lokalen Server auftritt.

**Die Ursachen ermitteln**

Bei großen IT-Infrastrukturen und ebensolchen IT-Abteilungen gibt es immer mal wieder die Tendenz, das Problem andernorts zu vermuten. Wenn beim Helpdesk Klagen über eine langsame Anwendung eingehen, verweist der Systemadministrator schon mal auf Netzwerkprobleme. Das Netzwerkadministrator verortet seinerseits die Probleme im Bereich Storage. Der Storage-Verantwortliche gibt hingegen der Anwendung selbst die Schuld. Bei vagen Symptomen, wie einer langsamen Anwendung, gilt es zunächst zu identifizieren, wo genau im Rechenzentrum das aktuelle Problem zu verorten ist. Sind mehrere Server und Anwendungen betroffen, weist dies eher auf Netzwerk- oder Storage-Probleme als auf ein eigentlichen Serverfehler hin. Bei virtualisierten Umgebungen sollte der physische Standort der betroffenen VMs (virtuelle Maschinen) überprüft werden, um sicherzustellen, dass nicht alle dieselbe, möglichweise beeinträchtigte, Hardware nutzen.

Das Ausschlussverfahren hilft dabei, das eigentliche Problem enger einzukreisen. Das klappt nicht immer auf Anhieb und kann sich ebenfalls komplex gestalten. Man kann dabei unterschiedliche Faktoren kombinieren, um die möglichen Ursachen einzugrenzen.

**Dokumentation richtig einsetzen**

Da in der Known-Error Datenbank keine weitere Ursache dokumentiert wurde, kann man hier nicht viel mit der Dokumentation arbeiten.

**Richtig kommunizieren**

Die richtige Kommunikation kann oft der Schlüssel zur Problemlösung sein. Wenn ein Kollege am Vorabend eine Servereinstellung geändert hat, und am nächsten Morgen eine Anwendung nicht wie gewohnt funktioniert, kann die Ursache unter Umständen sehr schnell gefunden werden.

**Überwachung und Monitoring**

Wenn aussagekräftige und aktuelle Informationen zum Betrieb des Rechenzentrums vorliegen, lässt sich das Problem häufig schnell lokalisieren und lösen. Entsprechende Tools fürs Monitoring existieren für alle Größen und Strukturen von Rechenzentren. Wenn diese Tools alle wichtigen Kennzahlen ständig erfassen, weiß man von Anfang an, ob man sich an den Netzwerkadministrator oder an den Storage-Verantwortlichen wenden muss. Zudem liefern diese Werkzeuge Informationen, die IT-Abteilungen bereits auf künftige Probleme hinweisen, so dass es für den Anwender gar nicht erst zu einem spürbaren Fehler kommt, sondern diese vorab vermieden werden kann.

4) Nennen und erläutern Sie mögliche Fehlerquellen und erläutern Sie Maßnahmen zur Beseitigung

**1. Möglichkeit**

Dieses Verhalten kann auftreten, wenn die Verbindung mit dem Netzwerkspeicherort während des Öffnens der Datei durch ihr Office Programm unterbrochen wird.

Diese Situation kann auch auftreten, wenn die Verbindung mit dem Netzwerk langsam ist, da das Office Programm mehrere Abfragen an das Netzwerk durchführen muss, um die richtigen Dateiinformationen abzurufen.

**2. Möglichkeit**

Bei der Installation ist ein Fehler unterlaufen, die Verwendung auf Excel durch Fernzugriff funktioniert daher nicht immer und wirf Fehlermeldung. Die Fehlinstallation kann auch ein Update verhindern, welches die Performance und der Applikation behindert.

Die Applikationen neu installieren und prüfen, ob die Applikation richtig installiert wurde.

**3. Möglichkeit**

Es kann auch sein, dass ein Virus irgendwo heruntergeladen wurde und das System von innen manipuliert und blockiert. Der Virus könnte die Daten verschlüsseln oder sperren, was die Frage auf die Verfügbarkeit der Daten aufweist.

Den Virus so schnell zu entdecken und entfernen. Den Auslöser des Virus identifizieren und dokumentieren.

**4. Möglichkeit**

Das Netzwerk wird von außen attackiert, welches die Performance verschlechtert und die langsame Reaktionszeit der Applikation erklärt. Ein Hacker-Angriff kann auch der Grund dafür sein, dass die Daten gesperrt und nicht zugänglich sind.

Ersten soll alles gesichert werden was geht und dann den Strom abschalten, damit kein weiterer Schaden angerichtet werden kann. Dann hilft es die Polizei anzurufen und nächste Schritte zu planen, oder auf die Bedingungen der Angreifer einzugehen und zu hoffen, dass die Daten zurückgegeben werden.