Ingenieurbüro Kaufmann

Christof Kaufmann

Diplom-Ingenieur **Graduate Engineer**

Maschinenbau **Mechanical Engineering**

kaufmann@ibkaufmann.com

IT Memo

Im Unternehmen besteht in den meisten Situationen (Zugriff auf Files, Kalkulationen, Emails, andere Dokumente, Buchungssysteme, DMS, CMS , ERP, SAP-Einsatz etc.) eine Client-Server-Struktur. Nicht unter diesen Begriff fallen zum Beispiel spezielle Arbeitsplätze für die Software-Entwicklung, hardwaregebundene Programmierplätze für CAD/CAM-Lösungen, Maschinen-und Anlagensteuerung und dergleichen, wobei bei den letzteren die Frage ist, ob hier nicht bereits der Hersteller den Programmierplatz passend und vor allem zwingend zur Maschine bereitstellt. Aber grundsätzlich ist es auch hier möglich, etwa ein Maschinensteuerungsprogramm am PC zu entwickeln und anschließend auf die Maschine zu laden. Gerade bei Simulationsprogrammen für Steuerungen ist dies regelmässig der Fall.

Betriebssysteme für Rechner stammen auch heute noch nicht grundsätzlich von Microsoft, aber eben sehr häufig und das hat seine Gründe: Apple hat seine Systeme nie wirklich für den Einsatz im Netzwerk konzipiert. Es gibt zum Beispiel keine Server von Apple. Bei LINUX als UNIX-Derivat verhält sich das ähnlich. Beide Produkte können zwar durch bestimmte Maßnahmen „netzwerktauglich“ gemacht werden, sowohl als Server als auch als Client, aber dies ist eher als Nothilfe im Einzelfall zu verstehen. Eine Lösung im eigentlichen Sinne ist das für den professionellen Einsatz im Unternehmen nicht. Mit Lösungen wie etwa die SUN Workstation aus den USA liegen hier keine Erfahrungen vor. Das sind komplett eigene Systeme mit ganz bestimmten Aufgaben.

Serverbetriebssysteme kommen heute hauptsächlich von Microsoft und (allgemein etwas weniger bekannt) nach wie vor von IBM.

Microsoft Upgrades für Server: Auch hier hat MS die Unart entwickelt, neue Betriebssystem-Versionen in immer kürzeren Zeitabständen zu veröffentlichen, was gerade Vertragskunden in die Pflicht zwingt, in immer kürzeren Abständen praktisch die komplette Server-Landschaft zu erneuern. Erschwert wird das dadurch, dass in der Regel ein einfach zu handhabendes generelles Versionsupgrade nicht zur Verfügung steht, obwohl dies formal behauptet wird. Führt man es aus, wird man feststellen, dass man danach eine leere, quasi auf Anfangszustand zurückgesetzte Maschine hat, was nicht dem erwarteten Sinn entspricht. Zudem ist nicht jede herausgegebene neue Version ein Gewinn ! Das Betriebsystem Server 2008R2 war eine gute stabile Plattform, dies trifft auch auf Server 2019 zu. Die Versionen dazwischen (Server 2012 und Server 2016) brachten manche Schwächen mit sich und müssen als nicht ausgereift betrachtet werden. Im Grunde sind das Entwicklungsversionen auf dem Weg zu Server 2019, die aber vorzeitig verkauft wurden.

Microsoft Updates für Server: Bei der Flut der veröffentlichten Updates gibt es das Problem, dass diese Updates zwar automatisch heruntergeladen werden können, aber nicht automatisch installiert werden. Diese Einstellung gibt es nicht, manuelles Eingreifen ist erforderlich. Dazu kommt, dass meist ein Neustart erforderlich wird, der aber nicht selten dazu führt, dass Dienstprogramme –obwohl sie auf automatischen Start gestellt sind- eben nicht starten. Das hat den Hintergrund, dass bei Start nach Update der Server noch einen guten Teil des Updates zu verarbeiten hat und dabei einfach „vergisst“, dass da noch ein paar Dienste gestartet werden müssen. Auch hier muss manuell eingegriffen werden. Bei kleinen Netzen mit 10 Servern ist das Problem klein. Bei großen Netzen mit >100 Servern ist das Problem groß. Wohl gibt es das netzwerkweite Update Deployment, aber das ist keine große Hilfe, denn damit sind die Updates zu den Zielmaschinen zwar deployed, aber noch immer nicht installiert und das Problem mit ggf. nicht startenden Diensten bleibt.

Diese Probleme hat ein Kunde nicht, dessen Basismaschinen im Serverbereich nach wie vor ältere Betrienssysteme besitzen wie Server 2003 oder Server 2008R2 und nur dort einen Server 2019 einsetzt, wo er aus funktionalen Gründen auch wirklich gebraucht wird. So ist es zum Beispiel völlig unnötig, einen Domaincontroller auf Basis Server 2008R2 durch einen Server 2019 zu ersetzen, nur weil Microsoft das gerne so hätte. Auch ansonsten ist der Begriff der Notwendigkeit zu hinterfragen: grundsätzlich verhält sich Microsoft nicht offiziell abwärtskompatibel. Der Versuch aber zeigt in vielen Fällen, dass etwa

auf Server 2019 auch Programme einwandfrei laufen, die für Server 2008R2 entwickelt wurden (z.B. Microsoft Office 2010) und umgekehrt ein Programm, welches nach Herstellerangabe „ab Server 2019“ freigegeben ist, problemlos auf Server 2008R2 läuft. Aber es kann tatsächlich der Fall eintreten, dass eine Software, die auf 2008R2 noch lief, unter Server 2019 neu programmiert werden muss, weil Microsoft zu viel verändert hat. Worin natürlich eine gewisse Absicht liegt.

Microsoft-Netzwerke sind zunächst einmal relativ einfach zu verwalten, sofern es sich um ein LAN mit weniger als 254 Einheiten (meint Computer und Drucker usw.) handelt, was mit einem „einstufigen“ IP4-Netz abgebildet werden kann. Werden es mehr als 254 Einheiten, muss das Netz segmentiert werden und es kommt zur Definition von Überleitungen und Weiterleitungen. Bis zu 500 gleichzeitigen Logins arbeiten Microsoft Netzwerke relativ unproblematisch. Darüber hinaus –etwa bei einer Fluglinie mit 5.000 gleichzeitigen Logins- kommen Schwierigkeiten hoch, die spezielle Maßnahmen erfordern.

Cloud und Server in der Cloud sind eine Modeerscheinung, die vor allem mit scheinbar billigen Preisen lockt. Sie sollen wie nicht anders zu erwarten natürlich die Kasse der Anbieter füllen. Wenn man genauer hinsicht, stellt man fest: der Administrator des Kunden kann diese Server nicht uneingeschränkt verwalten, es gibt nicht unterstützte Features im Zusammenhang gerade mit eigener Software und man kann kundenseitig diese Server nicht zu einem Netz verbinden. Im Ergebnis fängt auch schon ein kleineres Unternehmen, welches vielleicht nur 5 Server braucht, damit schlicht nichts an. Abgesehen davon befinden sich die Unternehmensdaten außer Haus = Sicherheitsaspekt. Etwas anderes ist es, Sicherungen in einer Cloud abzulegen. Da eine „Cloud“ aber nichts andres ist als ein Verkaufsbegriff für ein webdav-gestütztes SSL-Remote-Laufwerk, kann der Kunde dies genau so gut mit eigenen Mitteln erledigen. Dazu braucht er keinen Anbieter.

Virtualisierung von Servern (und auch Arbeitsplätzen) kommt dem heutigen Kunden gerade unter dem Aspekt der Kosteneinsparung bereits sehr entgegen: auf einer einzigen Hardwareplattform, die mit 350 GB RAM ausgestattet ist, laufen problemlos 15 Microsoft Server (oder anderes) als „virtuelle Maschinen“ („VMs“). Kurz nach dem Jahr 2000 wurde die Technik der Virtualisierung von VMware zuerst als Testszenario für die Entwicklung von Betriebssystemen entwickelt. Mit dem Produkt HyperV hat Microsoft – wie so oft- erst nachgezogen. Beide Produkte sind ausgereift und zu empfehlen. Was den RAM-Bedarf einer einzelnen VM anbel angt, neigen gerade die jüngeren Administratoren zur starken Übertreibung, was dann zu einer scheinbaren RAM-Knappheit führt. Erfahrene beginnen mit einem kleinen Wert, schauen sich dann die Maschine im Betrieb an und regeln sie so ein, dass der als frei gemeldete RAM im Betrieb ca. 40% des zugeteilten RAM entspricht. Das genügt völlig. Und so stellt man dann fest, dass z.B. statt 64 GB RAM „*nach Empfehlungen*“ bereits 8 oder 10 GB völlig genügen.

IT-Sicherheit ist ein sehr komplexes und umfangreiches Thema, welches daher hier nur ansatzweise behandelt werden kann. Und es ist so, dass die Notwendigkeiten aufgrund möglicher Gefährungen bei einem kleinen Privatgewerbe ganz anders zu bewerten sind als im Bank- und Börsenwesen oder im Bereich großer Firmen oder der Kritischen Infrastruktur (Kraftwerke, Leitstände, Rüstung, Militär, Polizei und Rettungsdiensten) Grundsätzlich unterschieden wird zwischen der Gefahr von außen und der Gefahr von innen, wobei zum Letzteren auch schlicht die Ahnungslosigkeit oder Schusslichkeit von Mitarbeitern zählen kann. Grundsätzlich gilt: ein Netz, das man von außen nicht sieht, kann man von außen auch nicht angreifen ! Man unterscheidet in der IT die „gute“ und „böse“ Seite. Während der gute Administrator für die gute Seite verantwortlich ist, also für das Funktionieren des Netzes und der Infrastruktur insgesamt und hierfür Fachmann ist, ist der der „böse ITler“ Fachmann für die andere Seite: er hat die Techniken des Eindringens, Mitlesens, Stehlens oder Zerstörens erforscht und ist dort Fachmann. Gut beraten ist ein Kunde, dessen fähiger Systemadministrator mit einem Fachmann für die böse Seite, in Deutschland etwa dem Hamburger Computer Chaos Club, Kontakt aufnimmt und sein System von außen prüfen lässt. Selbstverständlich sind unbesonnen geöffnete Emails in der Praxis die häufigste Ursache für Gefährdungen und tatsächliche Schadenfälle, aber es gibt auch dokumentierte Angriffe, die über eine Schwachstelle im Treiberprogramm für einen Festplattencontroller erfolgten. Eine derartige Gefahr kann nur von einem Spezialisten entdeckt werden. (Wenn überhaupt! Letzere Hürde gilt Gott sei Dank aber auch für den Angreifer!)

Fernzugriffe via VPN aufs Firmennetz haben sich als insgesamt sichere Lösung etabliert. Der Aufbau einer VPN-Verbindung mit einer Verschlüsselungstiefe von 1024 bit kann auch heute noch für die meisten Fälle als genügend abhörsicher angesehen werden. Aber mehr ist natürlich immer besser. Zudem empfielt sich eine Lösung, die nur Verbindungen zwischen definierter Hardware, also zum Beispiel der Firewall des Unternehmens zu bestimmten Rechnern zuläßt. Hierbei wird zur Identifikation die stets eindeutige MAC-Adresse des zugreifenden Rechners benutzt.

VPN für internationale Verbindungen ist etwas anderes und läuft über Provider mit einem eigenen Servernetz im entsprechenden Land. Für vielreisende Geschäftsleute, Journalisten und einfache Touristen ist der Aufbau einer Verbindung zur Heimat in manchen Ländern nur unter Nutzung solcher providergestützen VPN-Verbindungen möglich. Über Sinn, Unsinn und vor allem der Berechtigung für meist

staatlich angeordnete Beschränkungen läßt sich streiten. Oder man löst das Problem schlicht. Auch ein deutscher Reisender kann im Ausland etwa die deutsche Sportschau als öffentliches Angebot der deutschen ARD ohne einen solchen VPN nicht genießen. Auch die Anmeldung an (Email)Konten kann im Ausland ohne einen solchen VPN Schwierigkeiten machen oder stellt ein Sicherheitsproblem dar.

Microsoft RDP-Protokoll für Terminalserver-Sitzungen galt in früherer Zeit als sicher, da es seine eigene Verschlüsselung mitbringt. Diese Information ist aber mittlerweile hinfällig. Der Schlüssel ist zu schwach und das RDP-Protokoll hat aufgrund seiner Funktionalität zu viele Löcher, die für einen Angriff auf die Zielmaschine genutzt werden können. So sollte das für die Arbeit äußerst praktsiche RDP-Protokoll nur für Zwecke innerhalb eines LAN eingesetzt werden. Dort allerdings leistet es ausgezeichente Dienste: es ersetzt auch in Netzen mit vielen Mitarbeiter die Arbeit, Installatiionsmaßnahmen auf allen Arbeitsplatzrechnern einzeln durchzuführen. Der Administrator kann sich auf die Wartung der Terminalserver beschränken. Das Mapping des lokalen Druckers funktioniert in aller Regel ohne Treiberinstallationen. Für die Notwendigkeit von mehreren 100 gleichzeitigen RDP-Sitzungen gibt es bei Microsoft das sog. RDP-Farming, welches zwischen mehreren Terminalservern Load Balancing macht, um Leistungseinbrüche einzelner Server zu vermeiden. Heute ist ein Terminalserver nichts anderes als ein normaler Server, auf dem die sog. RDP-Dienste gegen Lizensierung einer bestimmten Anzahl von Sitzungen freigeschaltet sind. Leistungsstarke Anwendungen wie CAD oder Videoproduktion gerade mit starken Grafikanforderungen wird man nach wie vor an einem entsprechend ausgestatteten Arbeitsplatz ausführen und nicht in einer Terminalserversitzung. Auch für MAC Rechner von Apple gibt es taugliche RDP-Clients zum Zugang auf einen Microsoft Terminalserver.

Firewall ist ein Begriff, der in unterschiedlicher Bedeutung verwendet wird. Zum einen gibt es die **Rechner-Firewall**, mit der sich der Rechner / Server selbst schützt und dabei Regeln für eingehenden und ausgehenden Verkehr anwendet. Wesentlich bedeutender ist die **Netzwerk-Firewall**, welche zwischen dem externen Netz / WAN = Internet = Gefahr (Red) und dem internen Netz / LAN /(Green) und einem Mittelding dazwischen mit dem Namen DMZ = Demilitarisierte Zone und je nach Ausstattung auch noch weitere Netzsegmente. Eine gute Netzwerk-Firewall erlaubt es, den kompletten Datenverkehr zu überwachen und zu steuern. Regeln bestimmen, welche Anfragen aus einem der Segmente ggf. wohin weitergeleitet werden. Sie gibt die für einen VPN-Zugang notwendigen Zertifikate aus. Sie kann mit anderen –i-d.Regel baugleichen- Firewalls eine direkte Netz-zu-Netz-Verbindung herstellen. Sie kann auch als DHCP-Server fungieren und dynamische IP-Adressen vergeben. Befriedigend-gute Firewalls gibt es bereits kostenlos als Softwarevariante. Man kann ein definitiv sehr gutes Hardware-basiertes Gerät eines renommierten Herstellers aber auch für 5.000 Euro erwerben.

IP4- und IP6-Adressen : Während insbesondere für den internen Gebrauch im Firmen-LAN klar erkennbare IP4-Adressen nach dem Muster 192.168.020.001 sinnvoll sind, erweist sich eine IP6-Adresse nach dem Muster 2dfc:0:0:0:0217:cbff:fe8c:0. schlicht als unleserlich und damit äußerst schwer in der praktischen Handhabung, zumal sich 100 Rechner in einem Netz jeweils völlig anders darstellen und keinem erkennbaren Muster folgen. Das Argument für die Einführung von IP6 liegt in der explosionsartigen Vermehrung notwendiger IP-Adressen im öffentlichen Internet-Raum, verursacht insbesondere durch Handys und Tablets. Zum Status quo ist aber festzustellen, dass sich der IP6-Standard nicht durchgesetzt hat und eine schnelle Änderung ist nicht zu erwarten. Der IP6-Standard hat hauptsächlich den Ansatz, den Rechner weltweit einzigartig zu machen (ähnlich wie bei der MAC-Adresse) und damit sowohl Behörden als auch feindlichen Angreifern ein stets eindeutig definiertes Ziel bietet. Wir schalten so etwas konsequent ab.

Netzgeschwindigkeiten sind ein großes Thema, seit Glasfaserkabel (LWL) aufgekommen sind und Fiber To The Home (FTTH) ein Schlagwort geworden ist. Um das bewerten zu können muss man zunächst folgendes wissen: im optimalen Bereich der kurzen Kabelwege bis 250m, also im Firmen-LAN gab es die Sprünge von 10 Mbit/s auf 100 Mbit/s und danach auf 1 GBit/s = 1.000 Mbit/s, also nach den Zahlen jedes Mal eine Steigerung um den Faktor 10. Reale Messungen mit der Stoppuhr beim Übertragen definierter Datenpakete ergaben in beiden Fällen aber nicht den Faktor 10, sondern den Faktor 2,5 als reale Geschwindigkeitssteigerung. Wenn also an einem Standort eine 10 Mbit/s-Leitung mit Kupferkabel besteht, sollte man seine Erwartungen in Grenzen halten, wenn ein Anbieter „schnelle Glasfaser“ anbietet, sein Angbot im Kleingeruckten aber auf 100 Mbit/s begrenzt, aber den fünffachen Preis verlangt. Und eine stabile 10 Mbit/s-Leitung ist im Ergebnis mehr wert als eine wackelige 100 Mbit/s-Leitung mit Aussetzern. Lichtwellenleiter können unterwegs nicht durch Magnetsensoren einfach abgehört werden. Zugehörige zum Bereich Kritischer Infrastruktur benötigen eigene Kabel. LWL-Kabel können leicht 1.000 Mbit/s und mehr. Aber der Datenstrom muss auch verarbeitet bzw. in Empfang genommen werden und gerade an dieser Stelle ist häufig zu beobachten, dass durch Vollaufen von Buffern die Geschindigkeit bei großen Übertragungen nach einigen Sekunden nach unten geht.

SAP ist ein Unternehmen das im Ruf steht „einmal SAP, immer SAP“ und zudem die Geschäftsstrategie vertritt, nicht das SAP-Produkt müsse sich den Prozessen des Kunden anpassen; vielmehr müsse der

Kunde seine Prozesse an SAP anpassen. Zunächst erhält der Kunde ein Angebot für ein System. Was ihm nicht dazu gesagt wird, ist, dass er dasselbe System noch einmal für die Schritte der Entwicklung und den anschließenden Versuch braucht, im Ergebnis den 3fachen Preis bezahlt. Zumindest war das in der Vergangenheit so. Es gab 10 Mio.-Projekte, die rückabgewickelt wurden, weil SAP schlußendlich nicht in der Lage war, die Anforderungen des Kunden zu erfüllen. Der Grund dafür ist in der Struktur zu finden, wie SAP Kundenprojekte entwickelt. Das Stammhaus liefert 3 Basismodule, während sog. SAP-Berater –darunter sind auf einzelne Module spezialisierte Software-Häuser zu verstehen- die Module liefern, welche der Kunde tatsächlich benötigt. Tritt nun der Fall ein, dass der Kunde die drei Basismodule aus dem Stammhaus und zwei weitere spezielle Module aus zwei unterschiedlichen Software-Häusern benötigt, ist keinesfalls sichergestellt, dass das Ganze –da aus verschiedenen Quellen stammend- zusammen läuft. Und SAP selbst hat ein Problem damit, Updates für seine drei Basismodule herauszugeben, denn es ist nicht sicher, ob diese zusammen mit den Modulen der Software-Häuser sauber laufen werden. Untersuchungen zeigen, dass sich die IT-Kosten nach Einführung von SAP verdreifacht haben. Zumindest vor einiger Zeit war es so, dass SAP nicht öffentlich, aber im Hintergrund damit begonnen hat, seine Produkte von PC-basierten Microsoft Servern auf die Plattform AS00 / iSeries von IBM umzustellen. Auf diese Weise würde man auch ganz elegant das Update-Problem los.

IBM AS400 / iSeries ist eine schon vor langer Zeit (60er Jahre) entwickelte Lösung aus dem Bereich der sog. Mittleren Datentechnik und war ursprünglich für den Einsatz zusammen mit Hunderten von einfachen Terminals vorgesehen, die über einfache Telefondrähte mit der Maschine verbunden waren. Kennzeichen dieser Maschinen war von je her eine absolute Stabilität und das ist bis heute geblieben. Alle Prozesse laufen auf der Maschine selbst, der Zugriff erfolgt heute über Windows-Clients statt den Terminals. Es handelt sich um ein Baukasten-System, welches als kleinste Variante einen einfachen 19“-Einschub 3 HE darstellt, in einer starken Variante aber einen ganzen Raum füllt. IBM hat diese Serie immer weiter entwickelt und breits die Grundausstattung des IBM Betriebsystem Release bietet wirklich alles auch an modernen Features, was das Herz behehrt. Zur Grundausstattung gehört die IBM Datenbank DB2, die auch nach aktuellen Rankings zusammen mit ORACLE zu den weltweit schnellsten Datenbanken gehört. Im Vollausbau kann die Maschine 8 TB RAM (!!) verwalten. PC-basierte Maschinen können mit maximal ein paar Hundert GB hier nicht mithalten. Für die AS00 gibt es weder Updates (also auch keine notwendigen Neustarts) noch Viren oder Schadsoftare. IBM garantiert 100% Abwärtskompatibiltät, wenn irgendwann eine neue Maschine mit einem neuen Betriebssystem-Relase kommt. Große weltweit aktive Firmen wie TUI oder Airlines mit ihren Login-Anforderungen setzen die AS00 ein. Der einzige „Nachteil“ dieses Systems besteht darin, dass man –wie für jedes System- Programme dafür schreiben und auch pflegen muss.

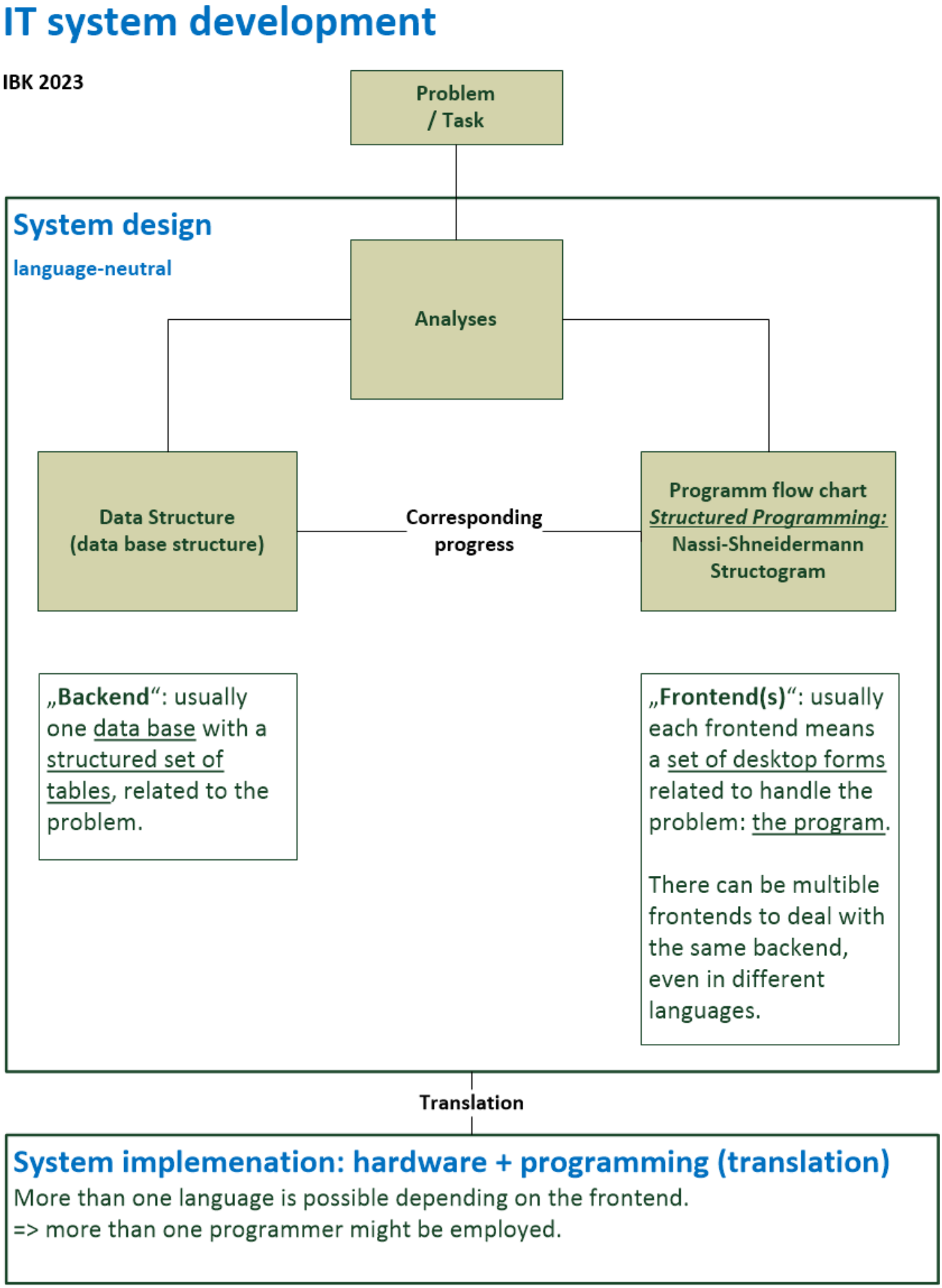
Datenbanken kommen für den großem Bedarf von **ORACLE** oder **IBM** je nach Hardwareplattform PC oder AS400, für den kleinen bis mitleren Bedarf von **Microsoft** als Microsoft SQL Server oder für den kostenlosen ganz kleinen Bereich als **MySQL**, beliebt als Internet-Datenbank. Heute unter Bezeichnungen wie ERP-, CMS- oder DMS-System erhältliche Systeme oder auch Buchführungs-/Finanzsysteme sind **Datenbankanwendungen** (**Frontend**), die auf eine speziell designten **Datenbankstruktur im Backend**, also auf dem Server laufend, zugreifen.

Hardwarenahe Programmierung, wie sie etwa bei Maschinensteuerungen und Simulationsprogrammen benötigt werden, ist ein völlig eigenes Thema. Hier kommt es vor allem auf Geschwindigkeit an: das Programm muss immer schneller sein als die Maschine laufen kann und die Simulation muss Massenträgheiten berücksichtigen. Sofern der Hardwarelieferant nicht bereits Vorgaben gemacht hat, kommt an dieser Stelle die hardwarenahe Programmiersprache **ASSEMBLER** bevorzugt zum Einsatz.

Softwareentwicklung: Jede vernünftige Programmierung folgt der Methotik des von **Nassi-Shneidermann** entwickelten allgemein gültigen Struktograms zur Darstellung der sog. *Strukturierten Programmierung*: im Plan aufgezeichnet werden einzelne Module, von denen jedes von oben nach unten durchlaufen wird und dabei stets einen definierten stabilen Endzustand erzeugt. Diese Darstellung ist programmiersprachenneutral und damit allgemein gültig. Sie kann anschließend in eine beliebige Sprache übersetzt werden. Dabei ist es durchaus möglich, einzelne Module in verschiedenen Sprachen zu realisieren. Unter Namen wie ***Scrum*** oder ***Agile Programmierung*** bekannt gewordene Herangehensweisen sind eher als Lehrmethoden zu verstehen, um im Ergebnis genau das Vorbeschriebene zu tun. Anders ausgedrückt: wer Nassi-Shneidermann wirklich verinnerlicht hat und so denkt, hat von Scrum etc. keine zusätzlichen Vorteile mehr.

Software mit direktem Zugriff: Das Internet ist als Netzwerk zu verstehen, über welches genau wie in einem LAN zum Beispiel auf eine Datenbank zugegriffen werden kann. Wir haben mit unseren Entsicklungen gezeigt, dass es gelingt, ohne Abstützung auf einen sicherheitsanfälligen WEB Browser gelingt, schlanke schnelle Software zu schreiben, welche einem Rechner mit beliebigem Standort die Arbeit auf dem Firmensystem gestattet ohne irgendwelche „Drittmittel“ dazwischen. Selbstverständlich abhörsicher.

Systementwicklung in der IT: das nachfolgende Bild zeigt die grundsätzliche Vorgehensweise bei der Entwicklung eines IT-Systems, welches bestimmte Aufgaben erfüllen soll.



Die durchaus nicht unkritische Idee von SCRUM ist nun, den ersten Schritt des *System Designs* bei größeren Projekten auf eine durch den *Scrum Master* moderierte Gruppe mehrerer Personen aufzuteilen.