April 2022

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Kritische Infrastrukturen und IT-Ausstattung

von Oliver Flüs
Ausgehend von der „Königsklasse“ Kritische Infrastrukturen will dieser Artikel Denkanstöße und Beispiele geben sowie auf nützliche Quellen hinweisen. Hintergrund sind ComConsult-Erfahrungen rund um kritische IT, aus KRITIS- und nicht-KRITIS-Umgebungen.

Fällt IT aus Sicht des Kerngeschäfts oder wichtiger Versorgungsketten länger aus, kann sich das kritisch auswirken.

Seite 8

Sind wir reif für IT-Mündigkeit?

von Dr. Behrooz Moayeri
In den letzten zwei Jahren hat sich die Art und Weise der dienstlichen Nutzung von IT grundlegend geändert – zumindest an denjenigen Arbeitsplätzen, die gezwungenermaßen von den Räumlichkeiten der Unternehmen in die privaten Haushalte verlagert wurden.

Seite 2

FOSS – Free and Open Source Software, eine Alternative

von Markus Geller
Das CERN hat Anfang 2019 ein Projekt auf den Weg gebracht, um die Abhängigkeit von Microsoft-Produkten zu minimieren. Jetzt liegen erste Erkenntnisse vor, die beschreiben, wie auch große Organisationen vom Einsatz der FOSS-Lösungen profitieren können. Die Überlegungen zu diesem Beitrag liegen also schon eine Weile zurück.

Seite 26

Webinar der Woche

Beteiligung des Betriebsrates bei der Einführung von Software

Seite 25

Halb kaputt ist meist schlimmer als ganz kaputt!

von Dr. Joachim Wetzlar
Neulich: Produktionsstillstand bei einem Industrieunternehmen. Wichtige Anwendungen zur Produktionssteuerung und Logistik waren „ausgefallen“. Genauer gesagt konnten die in der Produktion verteilten Clients ihre Server nur mit schlechter Performance und zum Teil gar nicht mehr erreichen. Aus Bürobereichen wurde überdies gemeldet, dass Dateizugriffe auf File Shares zum Teil nicht mehr möglich waren.

Seite 23

Sind wir reif für IT-Mündigkeit?

von Dr. Behrooz Moayeri

Fortsetzung von Seite 1

Auch wenn nun einige Beschäftigte wieder in die Bürogebäude zurückkehren, werden bei vielen Organisationen einige wegen der Pandemie erfolgte Änderungen in der IT-Nutzung nicht mehr rückgängig gemacht werden. Dazu zählt zum Beispiel die Nutzung virtueller Plattformen für Kommunikation und Zusammenarbeit (UCC). Damit geht in zahlreichen Fällen der direkte Cloud-Zugriff der Arbeitsplatzendgeräte aus dem Homeoffice einher. Diese Endgeräte, meistens PCs, kommunizieren häufig direkt mit Public Clouds, den Hosting-Umgebungen für UCC-Plattformen. Selbst wenn der Weg zu diesen Plattformen über ein Virtual Private Network (VPN) des Unternehmens und damit über das firmeneigene RZ führen sollte, können im Falle von UCC-Nutzung Firewalls und andere Sicherheitskomponenten in Firmen-RZs nicht viel kontrollieren. Deshalb haben einige Organisationen den kürzesten Weg von den Endgeräten zu den Clouds erlaubt, nämlich den Weg über das Internet – ohne VPN. Vor ein paar Jahren hätte das einer Vielzahl an IT-Sicherheitsverantwortlichen große Bauchschmerzen bereitet, und oftmals tut es das immer noch. Immerhin wird ein Endgerät direkt mit dem Internet verbunden. Bei Wegfall der Kontrollen, Einschränkungen und Sicherheitsmechanismen des Firmennetzes ist man wohl oder übel auf die möglichst sichere Konfiguration des Endgeräts UND die IT-Mündigkeit des Benutzers angewiesen. Letzteres bedeutet, dem Benutzer zuzumuten, dass er sensibilisiert genug ist, nicht etwa auf Phishing Mails reinfällt, nicht jede Web Page öffnet und bei nicht vertrautem Verhalten des Endgeräts und der Software innehält und wachsam bleibt.

Doch sind wir in diesem Sinne reif für IT-Mündigkeit?

Wachsende Bedeutung von Security Awareness

Voraussetzung für IT-Mündigkeit ist das Bewusstsein über die IT-Sicherheit, übersetzt Security Awareness. Ein solches Bewusstsein wird immer wichtiger. In den 1990er Jahren, als das World-Wide Web das Internet vom Medium für wenige zur wichtigsten Informationsquelle machte, habe ich dafür plädiert, dieses neue virtuelle Straßennetz wie das altbekannte zu behandeln. Das hätte bedeutet, dass Organisationen als Voraussetzung für den Webzugriff eine Art Internet-Führerschein eingeführt hätten. Das kann man auch Security Awareness nennen. Seit den Anfängen des WWW ist ein Vierteljahrhundert vergangen. Security Awareness ist noch wichtiger geworden. Deshalb wird meine Kollegin Dr. Stollenwerk auf unserer Sommerschule 2022 dazu einen Vortrag halten.

Es ist nicht unrealistisch zu erwarten, dass wir IT-mündiger und sicherheitsbewusster werden. Schließlich nutzt jede Person IT auch privat. Es ist nicht egal, ob unsere privaten Daten plötzlich von Ransomware verschlüsselt werden. Uns ist es wichtig, dass wir unsere Fotos und Filme aufbewahren und vor unbefugtem Zugriff schützen. Unser Online-Banking-Zugang ist ebenfalls sehr schützenswert. Genauso wie man die eigene Wohnung, das eigene Verkehrsmittel und die eigene Brieftasche nach Kräften schützt, muss man sich auch über den Schutz des eigenen PCs, des eigenen Smartphones und des eigenen Heimnetzes Gedanken machen. So entsteht automatisch mehr IT-Sicherheitsbewusstsein. Davon profitieren auch Organisationen, in denen die sensibilisierten Menschen arbeiten.

Nicht allein auf die IT-Mündigkeit setzen

Jedoch ist es verständlich, wenn viele Organisationen nach wie vor nicht allein auf die IT-Mündigkeit ihrer Beschäftigten setzen. Technische Vorkehrungen bleiben wichtige Komponenten des Schutzes der Ressourcen und der Daten von Organisationen.

Ein technischer Ansatz besteht darin, den Schutzwall um die Ressourcen und Daten der Organisation enger zu ziehen und alles außerhalb dieses Schutzwalls als nicht vertrauenswürdig zu betrachten („Zero Trust“). Dann sind die Endgeräte nicht mehr vertrauenswürdig, unabhängig davon, ob sie firmeneigene Endgeräte sind oder im Sinne von „Bring Your Own Device“ (BYOD) den Usern selbst gehören.

Setzt man konsequent auf Datenhaltung in eigenen oder Cloud-Rechenzentren, bedeutet Zero Trust gegenüber den Endgeräten,

Kritische Infrastrukturen und IT-Ausstattung

von Oliver Flüs

Fortsetzung von Seite 1

Bedrohungen durch Cyber-Kriminelle sind allgegenwärtig. Angriffe aus politischen Gründen machen immer wieder Schlagzeilen. Corona-Pandemie und jüngste Wetterkatastrophen haben gezeigt, dass solche Szenarien keine graue Theorie sind.

Besondere Absicherung ist schnell besonders teuer und aufwändig. Effektiver Schutz für Kritisches und Verhältnismäßigkeit sind schwer in eine gute Balance zu bringen.

Praxissicht zum Begriff „kritisch“ und zu Ketten schädlicher Folgen

Von kritischen Infrastrukturen war in letzter Zeit häufiger in der Tagespresse die Rede. Es handelt sich daher nicht länger um einen Begriff im Wortschatz von Spezialisten und Insidern. Warum kam es zu dieser verstärkten Erwähnung? Der Grund sind gefährliche Entwicklungen bei Rahmenbedingungen, deren Folgeschäden für die Bevölkerung und im täglichen Leben stark spürbar werden können oder geworden sind.

Ein in der Corona-Pandemie angefallenes Beispiel sind Engpässe bei Lebensmitteln und anderen Waren. Wegen der erhöhten Omikron-Ansteckungsgefahr wurden zudem vorsorglich Betrachtungen für Szenarien angestellt, bei denen durch hohe Kranken- und Quarantäne-Stände beim Personal Feuerwehren nicht in gewohnter Weise reagieren könnten, usw.

Die Besonderheit, weshalb solche möglichen oder tatsächlichen Engpässe Schlagzeilen machen, ist ein flächiges Auftreten. Auf leere Regale im einzelnen Supermarkt kann man als Kunde durch Einkaufen bei der Konkurrenz selbständig reagieren. Bei Ausfall einer einzelnen Feuerwache oder bei Personalengpass eines einzelnen Krankenhauses lässt sich organisieren, dass andere vergleichbare Einheiten zeitweilig übernehmen. Sind allerdings die Ausweichmöglichkeiten in einer bestimmten Gegend ebenfalls betroffen, wird es schwierig zu kompensieren: Eine ganze Infrastruktur zur Versorgung der Bevölkerung wird dann mindestens in einem bestimmten geographischen Gebiet am „Liefern“ gehindert.

Für die betroffene Bevölkerung gilt: Je näher der Mangel am täglichen Bedarf ist, umso stärker ist die Wirkung, wenn die übliche Versorgung nicht nur kurzzeitig eingeschränkt ist.

Die schädliche Wirkung kann sich durch Verkettung und Folgeschäden weiter verstärken. Fällt z.B. in einem Stadtgebiet für einige Zeit der Strom aus, passiert unter anderem Folgendes: Kühlräume und -theken setzen zeitweilig aus. Darin gelagerte verderbliche Lebensmittel tauen auf. Sie können je nach Fall nicht mehr ohne Gefahr für die Gesundheit der Kunden zum Verkauf und Verzehr angeboten werden. Bis Nachschub geliefert werden kann, besteht somit in der vom Stromausfall betroffenen Gegend bei solchen Lebensmitteln ein Engpass.

Beim planvollen Umgang mit derartigen komplexeren Szenarien tun sich selbst Profis aus dem Umfeld kritischer Infrastrukturen immer wieder schwer. Entweder ist das Denken über das auslösende Schadensereignis hinaus zu ungewohnt, oder man ist zu sehr auf die unmittelbar betroffene Technik fixiert. Außerdem schwingt verständlicherweise immer der Aspekt der Wirtschaftlichkeit mit. Verhältnismäßigkeit ist da ein schwieriges Ziel. Man schreckt vor dem Weiterdenken zurück.

Herausforderungen bei der technischen Konzeption und Betreuung einer virtuellen Konferenz

Mit Nils Wantia sprach Christiane Zweipfennig

Digitale Messen, virtuelle Konferenzen, Remote-Seminare – diese Begriffe sind spätestens seit dem Frühjahr 2020 in der Eventbranche nicht mehr wegzudenken. Damals häufig aus der Not heraus entstanden, erkennen Unternehmen heute zunehmend das Potential, das der virtuelle Raum für Veranstaltungen unterschiedlicher Art bietet.

Nils Wantia leitet bei ComConsult das Competence Center Kommunikationslösungen und erzählt in diesem Interview, wie er mit seinem Team am Anfang der Pandemie eine der ersten großen virtuellen Konferenzen technisch umgesetzt und begleitet hatte.

Im Sommer 2020 wurde ComConsult mit Beratungs- und Unterstützungsleistungen zur technischen Konzeption und Betreuung einer virtuellen Konferenz beauftragt.

Um welche Konferenz handelte es sich?

Es ging um eine internationale Konferenz, die immer als Präsenzveranstaltung stattgefunden hatte und nun erstmalig virtuell durchgeführt werden sollte. Die meisten der ungefähr einhundertzwanzig Teilnehmer waren „Stammgäste“ - über mehr als vierzig Länder weltweit verteilt - die sich seit ungefähr zwanzig Jahren regelmäßig auf der Konferenz getroffen haben, um sich untereinander auszutauschen und Fachvorträge zu hören. Der Großteil der Teilnehmer kam aus Nichtregierungsorganisationen, aus Deutschland waren auch Gäste von Behörden dabei. Wir wurden von einer kleinen Berliner Agentur beauftragt, die die Gesamtkoordination der Konferenz verantwortete.

Wie sah das Programm des Kongresses aus?

Die Konferenz war nicht öffentlich, die Teilnehmer wurden einzeln persönlich per E-Mail eingeladen. Der Kongress ging über zwei Tage. Der Ablauf hatte ungefähr dreißig Programmpunkte. Es gab jeden Tag zuerst ein Kaffee-Meeting zur Begrüßung, danach Instruktionen der Moderatoren und die Keynote. Danach fanden mehrmals große Gruppensessions statt, aus denen sich die Teilnehmer in eine von sechs parallel stattfindenden Breakout-Gruppen einwählen konnten. In diesen Untergruppen konnten die Teilnehmer dann miteinander reden und nach Bedarf wieder in die große oder eine andere kleine Gruppe wechseln. Am Ende der Veranstaltung fand eine sogenannte Fishbowl-Session statt, bei der eine kleine Gruppe von Teilnehmern in einer Art Podiumsdiskussion ein Thema diskutierte, während die anderen Teilnehmer zuhören und sich dynamisch in die Diskussion einschalten konnten.

Wichtig: Organisatorischer Mittelpunkt

Wer hat durch die Veranstaltung geführt?

Für die Veranstaltung war es wichtig, einen organisatorischen Mittelpunkt zu haben. Deshalb hatte die Agentur ein Filmstudio beauftragt, in dem professionelle Moderatorinnen von einem Podium aus die Veranstaltung von Anfang bis Ende begleiteten.

Halb kaputt ist meist schlimmer als ganz kaputt!

von Dr. Joachim Wetzlar

Fortsetzung von Seite 1

Eine erste Prüfung – nachdem ich mich über VPN mit dem Kundennetz verbunden hatte – ergab, dass die mir bekannten Subnetze in der Produktion allesamt erreichbar waren. Das Routing war aus meiner Perspektive unauffällig. Die IT-Abteilung vor Ort prüfte inzwischen verschiedene Meldungen im Netzwerkmanagement. Schließlich sagte einer: „Ich sehe bei einem Switch OSPF-Meldungen im Event Log!“

Das habe ich mir näher angesehen. Und richtig, alle paar Minuten meldete der Switch – ein Server Distribution Switch –, dass er einen benachbarten Router nicht mehr sehe. Jeweils kurz danach wurde der Router erneut erkannt, und so fort.

Wie waren die Kollegen vor Ort auf diese Meldung aufmerksam geworden? Im Netzwerkmanagement konnte man bei dem Switch ein kleines gelbes Dreieck erkennen, das auf einen „Minor Alarm“ hinwies. Auf einem Interface waren mehr fehlerhafte Pakete empfangen worden, als ein eingestellter Schwellwert zuließ. Die Prüfung ergab sehr schnell, dass es sich um genau dasjenige Interface handelte, auf welches sich auch die OSPF-Meldungen bezogen.

Was war zu tun, um den Fehler zu beheben? Wir haben einfach das betroffene Interface deaktiviert. Die Voraussetzung dafür war erfüllt, es gab eine Redundanz. Das Interface war eines von zweien, die den Server Distribution Switch mit dem Core verbanden. Nun wurden alle Pakete über dieses zweite Interface geroutet, das vermeintlich ohne Mängel war.

Ein gemeiner Fehler! Offensichtlich war ein Glasfaser-Transceiver defekt, sodass Pakete mit einer gewissen Wahrscheinlichkeit mit falscher Prüfsumme empfangen und also verworfen wurden. Das führte zu massiver Beeinträchtigung jeglicher Kommunikation über dieses Interface, wovon letztlich alle wichtigen Anwendungen betroffen waren.

Warum hatte das Routing-Protokoll OSPF die Verbindung nicht dauerhaft aus seiner Datenbank gelöscht? Das liegt an dem vielen Routing-Protokollen eigenen „Hello-Mechanismus“. Erst wenn mehrere Hello-Pakete in Folge verloren gehen, wird die Verbindung als inaktiv markiert.

Die Verkettung mehrerer Ereignisse führt zu einer Potenzierung der Wahrscheinlichkeiten. Nehmen wir die Paketverlustrate von 10% an. Dann beträgt die Wahrscheinlichkeit für den Verlust dreier aufeinanderfolgender Hello-Pakete $1/10^3$, also nur 0,1%.

Im Gegensatz dazu reicht der Empfang nur eines Hello-Pakets aus, damit das Routing-Protokoll die Verbindung wieder als aktiv markiert. Die Wahrscheinlichkeit dafür beträgt im genannten Beispiel 90%.

Fassen wir es noch einmal zusammen:

- Ein Glasfaser-Transceiver wird defekt und es entstehen Paketverluste.
- Die Paketverluste stören Anwendungen massiv.
- Die Redundanz wirkt nicht, weil das Routing-Protokoll die Störung kaum erkennen kann.
- Erst das Deaktivieren des Interface macht aus „halb kaputt“ ein „ganz kaputt“ und die Redundanz wirkt.

FOSS – Free and Open Source Software, eine Alternative?

von Markus Geller

Fortsetzung von Seite 1

Sie beruhen im Grunde auf drei Auslösern, die in den vergangenen Jahren aufgetreten sind:

- Kunden und Teilnehmer an Veranstaltungen der ComConsult Akademie erkundigen sich immer häufiger nach Alternativen zu den marktüblichen Produkten.
- Cloudlösungen werden hinterfragt, und Kunden wünschen Informationen zu Lösungen, die ohne die Public Cloud ebenfalls einsetzbar sind.
- 2019 stellte das CERN in Genf mit MAlt ein Projekt vor, welches die Möglichkeiten zur Ablösung von Microsoft-Lösungen in großen Umgebungen ermöglichen sollte.

Zu den ersten beiden Punkten werde ich im weiteren Verlauf einige Beispiele aus verschiedenen IT-Bereichen präsentieren.

Doch zunächst möchte ich das Projekt MAlt vorstellen und mit diesem Beispiel zeigen, dass sich auch große Organisationen von klassischen Softwareanbietern unabhängig machen können.

Das MAlt-Projekt

MAlt steht für Microsoft Alternatives und wurde aus einer für das CERN in Genf recht unbefriedigenden Situation heraus angestoßen.

Im Jahr 2019 wurde dem CERN, seitens Microsoft, der Status einer akademischen Institution entzogen. Dies führte zu stark steigenden Lizenzkosten für die vom CERN genutzten Microsoft-Produkte, da die günstigeren, akademischen Lizenzen nicht mehr zur Verfügung standen.

Über die Beweggründe von Microsoft kann man nur spekulieren, jedenfalls führte der Entzug des Status zu einem Umdenken, welches in der Vermeidung von Microsoft-Produkten mündete. (siehe Abbildung 1)

Dabei liegen die Haupterkenntnisse nicht in den alternativen Softwarelösungen, sondern vielmehr im organisatorischen Umdenken. Sechs Schlüsselfaktoren wurden ermittelt, die den zukünftigen Umgang mit Software erleichtern sollen [2]:

- Accounting: Die Kenntnis der mit Software verbundenen Gesamtkosten kann allen Beteiligten helfen, bessere, fundierte Entscheidungen zu treffen.
- Berechtigung: Auf der Grundlage des Accounting hat die IT-Abteilung gelernt, wie wichtig es ist, klare Berechtigungskriterien – basierend auf den Bedürfnissen – für lizenzierte Produkte zu definieren. Dadurch wird sichergestellt, dass die Kosten nicht automatisch stark anwachsen, wenn die Personalzahlen zunehmen.
- Standardisierung: Bei Standard-Produkten sollte auf Out-of-the-Box-Software gesetzt werden. Die Minimierung von Anpassungen dort, wo sie nicht unbedingt erforderlich sind, stellt sicher, dass die Services überschaubar und erschwinglich bleiben und einfach aktualisiert oder ersetzt werden können.
- Benutzereinbindung: Eine gute Kommunikation mit den Nutzern und eine abteilungsübergreifende Governance sollen der IT-Abteilung helfen, die Bedürfnisse zu verstehen und geeignete Software bereitzustellen.
- Architektur: Softwareprodukte sollten nicht unabhängig voneinander betrachtet werden, sondern als Teil einer soliden, nutzerzentrierten Technologielandschaft in der gesamten Organisation.