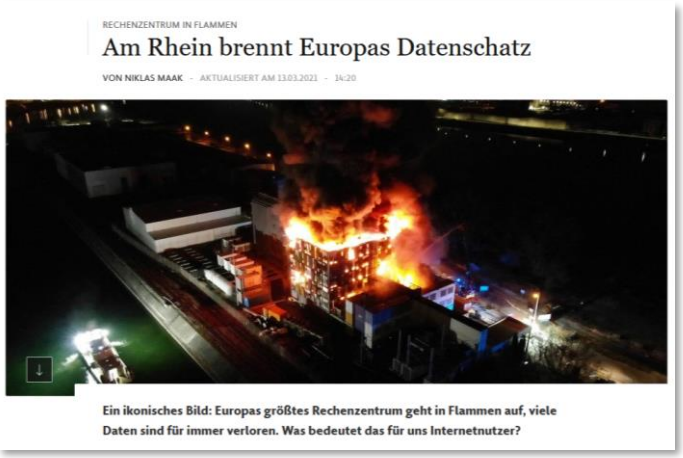
Herr Nettmann vom gleichnamigen Autohaus ist nach dem Lesen des nebenstehenden Artikels besorgt. Gerade der Fall, dass dadurch auch die Website seines Unternehmens längere Zeit ausfiel bereitet ihm Kopfzerbrechen.

Quelle: https://www.faz.net/aktuell/feuilleton/medien/groesstes-rechenzentrum-europas-brennt-komplett-nieder-17241629.html, 14.10.2021



RECHENZENTRUM IN FLAMMEN

Am Rhein brennt Europas Datenschatz

VON NIKLAS MAAK - AKTUALISIERT AM 13.03.2021 - 14:20

Ein ikonisches Bild: Europas größtes Rechenzentrum geht in Flammen auf, viele Daten sind für immer verloren. Was bedeutet das für uns Internetnutzer?

Welche Arten von Rechenzentren kann man unterscheiden?

Man unterscheidet zwischen externen und internen Rechenzentren, d. h. Rechenzentren von Dienstleistern (Cloud-Rechenzentren) und unternehmenseigene Rechenzentren (Inhouse Data Center, Enterprise RZ). Beide nutzen vergleichbare Rechneranlagen und Infrastrukturen.

Welche unterschiedlichen Arten von Service werden bei Cloud-Rechenzentren angeboten?

- Infrastruktur als Service (Infrastructure as a Service, IaaS) -> Sys Admins
  IT-Ressourcen wie Rechenleistung, Datenspeicher oder Netze werden als Dienst angeboten. Der Kunde kann darauf ein Betriebssystem mit Anwendungen seiner Wahl laufen lassen.

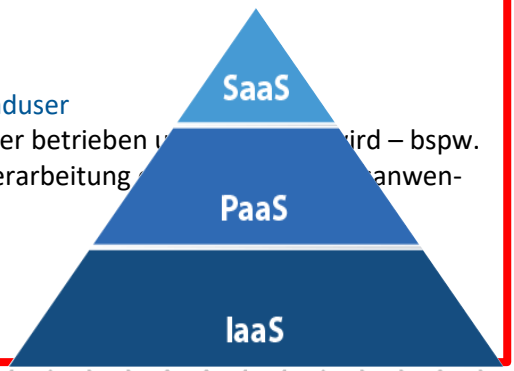
  Amazon AWS, HP Cloud, …

- Plattform als Service (Platform as a Service, PaaS) -> Software Developer
  Der Kunde hat keinen Zugriff auf das Betriebssystem und die Hardware, er kann aber auf der Plattform eigene Anwendungen laufen lassen.

  MS Azure, Google App Engine, …

- Software als Service (Software as a Service, SaaS) -> Enduser
  Zugriff auf ein Softwareprodukt, das vom Dienstanbieter betrieben u ird – bspw. Kontaktdatenmanagement, Finanzbuchhaltung, Textverarbeitung anwendungen.

  Gmail, Dropbox, …



Welche Bedrohungen können zu einem Serverausfall führen?

Interne Bedrohung (beeinflussbar)	Externe Bedrohung (nicht direkt beeinflussbar)
• Technischer Defekt (Software + Hardware) • Folgeschäden (Ausfall Klimaanlage) • Stromausfall • Schlechte Rahmenbedingungen • Fehlkonfiguration (falsches Rechtemanagement) • Menschliches Versagen	• Kriminelle Handlungen (Diebstahl von Hardware) • Malware (Viren, Trojaner, …) • Hacker (Fremdzugriff, DDoS) • Höhere Gewalt (Hochwasser, Brand, Erdbeben) • Ausfall des Internet-Providers

Welche Maßnahmen sollte ein Unternehmen ergreifen, um den Schutz vor Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Sicherheitsrisiken zu gewährleisten?

Zugriffsteuerung MitarbeiterSchulung	Infrastruktur(Raid) Firewall Virenscanner Feuerlöschsystem Aktuelle Updates(OS)	regelmäßige Backups USV
Vertrauliches (Confidentiality)	**Integrität (Integrity)**	**Verfügbarkeit (Availability)**
Infomationen sollen nur diejenigen erreichen, die diese Informationen auch besitzen dürfen bzw. vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden. Nur autorisierte Benutzer oder Programme dürfen auf die Information zugreifen.	Die Daten sind vollständig korrekt und unverändert. Integrität liegt vor, wenn Nachrichten unverändert übertragen bzw. zu-gestellt werden und Programme wie beabsichtigt ablaufen.	Autorisierten Benutzer stehen Daten bzw. Informationen aber auch Dienstleistungen bzw. Funktionen eines It-Systems zum gewünschten Zeitpunkt zur Verfügung.