Systemcrash

Markus Lehner, Infomail 1260, 22. Juli 2024

Am Freitag, den 19.7.2024, um 4 Uhr der globalen Computerzeit (UTC), kam es nach einem Softwareupdate weltweit zu einem Totalausfall zentraler Computersysteme. Infolgedessen wurden Flughäfen lahmgelegt, Zahlungssysteme stillgelegt, Krankenhäuser vom Netz genommen, Fernsehkanäle ausgeschaltet, Fabriken zum Stillstand gebracht – und vieles mehr. Nach dem Einspielen nur einer Datei als Fix des Problems war die Ursache zwar schon nach etwa einer Stunde behoben, allerdings dauerte es noch den ganzen Freitag und teilweise länger, bis die nachgelagerten Systemausfälle halbwegs überwunden waren.

Dieser Vorfall wirft ein Schlaglicht auf die Situation in den zentralen IT-Infrastrukturen, in denen sich in den letzten Jahren und besonders durch gegenwärtige Trends eine Menge neuer Risiken angesammelt haben. Hier ein paar dieser Beispiele und die Skizze einer Antwort aus marxistischer Sicht.

Wachstum und Monopolisierung

Ein wichtiger Trend hinter dem Vorfall ist sicherlich der qualitative Sprung in der Nutzung von Cloud-Computing, der sich in den letzten beiden Jahren nochmal verstärkt hat. D. h., immer weniger Firmen (egal welcher Größe) nutzen noch eigene Rechenzentren (mit Serversystemen vor Ort), sondern haben praktisch alle geschäftsrelevanten Backendprozesse in nur noch „virtuell“ eigene Teilbereiche von globalen Server-Betreiber:innen ausgelagert. Hier teilen sich eine Handvoll globaler Großkonzerne, wie Azure von Microsoft, die Google-Cloud von Alphabet, AWS von Amazon etc. den Markt auf. Laut de.statista.com stiegen die globalen Umsätze 2023 auf bereits 561 Milliarden US-Dollar und werden dieses Jahr 675 Milliarden erreichen. Zum Vergleich: Im Jahr 2020 lag die Zahl noch bei 270 Milliarden und vor 2015 war man noch unter der 100 Milliardengrenze. Dies spiegelt eine gewaltige Zentralisierung von Datenhaltung, Applikationsausführung und Dienstleistungen auf wenige IT-Betreiber:innen dar. Andererseits reduzieren diese wiederum ihre Kosten durch Auslagerung von Hardware und Dienstleistungen an Sub (-Sub-…)-Firmen. Dazu kommt, dass viele der Anwendungen „alt“ (im Sinne der IT-Entwicklungszeiten) sind und so ein Mischmasch an zum Teil nicht kompatiblen Systemen entsteht bzw. solche, die nicht wirklich cloudfähig sind, mit integriert werden müssen, so dass für solche Probleme eine Menge an Anpassungsebenen für den Weiterbetrieb eingeführt werden muss. Dieses ganze komplexe Gebilde erfordert einen hohen Planungs- und Betriebsaufwand – und sämtliche Änderungen an einer Stelle können schnell zu unübersehbaren Konsequenzen an anderen Orten führen.

Insbesondere aber stellt diese jüngste massive Verlagerungswelle in die Cloud neue Herausforderungen an die „IT-Sicherheit“. Dies betrifft nicht nur den gesicherten Datenzugriff (auch hochsensible persönliche Daten, z. B. zu Gesundheit oder sexueller Orientierung, lagern ja jetzt zumeist irgendwo auf der Welt in Cloudspeichern), sondern auch die Vermeidung von gravierenden Fehlern bei Applikationen oder Dienstleistungen (z. B. Schutz vor Ausfall von lebenswichtiger Infrastruktur). Es ist daher kein Wunder, dass der Markt von Cloud-Security-Produkten zu den am größten wachsenden Bereichen im an sich schon wachsenden Cloud-Sektor zählt. Laut Gartner waren 2023 an den Cloud-Verkäufen 32 % sicherheitsbezogen (gegenüber 13 % Anteil an Security bei sonstigen IT-Geschäften). Jüngstes Beispiel ist die Rekordübernahme des israelischen IT-Security-Startups Wiz durch Alphabet (Google) für 23 Milliarden US-Dollar – eine von etwa 50 Übernahmen von IT-Security-Firmen nur in diesem Jahr (laut JPMorgan Chase).

Diese IT-Security für Cloud-Systeme betrifft bei weitem nicht nur Firewall- oder Authentifizierungssysteme, sondern vor allem solche zur „präventiven Gefahrenabwehr“. Hier werden insbesondere die neuen AI-Systeme (Mashine-Learning, Language Modelling, generative und pre-trained Modelle etc.) als erstem großem kommerziellem Gebiet eingesetzt. Da dort die globalen Datenströme (und wohl auch Cloud-Inhalte) auf „sicherheitselevante“ Zusammenhänge durchforstet werden, lässt dies wenig Gutes für die viel versprochene Absicherung des AI-Gebrauchs in Bezug auf Datenschutz erwarten. Ein großer Teil der besonders heiß gehandelten Firmen wie Wiz oder Armo stammt aus dem Bereich der israelischen Streitkräfte (Security-Entwicklung aus Israel wird anders als bei anderen Herkunftsländern von der NSA von etlichen Einschränkungen ausgenommen) bzw. von ehemaligen Mitarbeiter:innen der US-Sicherheitsbehörden. Dies verheißt nichts Gutes für die von Snowden auf viel niedrigerem Entwicklungsniveau aufgedeckten Tendenzen.

Profitmacherei und Sicherheit

Das Wachstum des Marktes an Security-Produkten geht notwendigerweise einher mit einem ständigen Umbau und Updatechaos bei den betroffenen Cloud-Systemen. Kaum eine Woche vergeht, ohne dass grundlegende Änderungen über die Cloudsysteme der Welt geschickt werden. Auch bei dem Vorfall vom 19.7. wurde in einem System der Firma CrowdStrike (Falcon), das von einigen wichtigen Cloud-Anbieter:innen verwendet wird, ein Update scharf geschaltet, das den „Sensor“ in der Interprozesskommunikation (IPC) von Microsoft-Windows-Servern betrifft (d. h. hier werden Daten abgegriffen, die zwischen Applikationen in Laufzeit ausgetauscht werden). Da in dem Sensor-Update ein Programmierfehler enthalten war, führte dies zum Crash der IPC und mit dem Ausfall dieses wesentlichen Betriebssystemelements zum baldigen Absturz aller vom Update betroffenen Windows-Server weltweit. Durch einfachen Austausch nur einer Datei konnte das Problem dann aber auch sofort wieder behoben werden.

Der andere Trend, der durch diesen Vorfall aufgedeckt wird, ist die Situation in den IT-Firmen selbst. Längst sind IT-Abteilungen durch Outsourcing und globales Verschieben von Dienstleistungen zu unüberblickbaren Chaosfaktoren geworden. Das Wachstum an Komplexität der zu managenden Systeme entspricht in keiner Weise mehr ihrer Kapazität, diese noch zu betreuen. Die Auswirkungen von Updates, die Fehlervorsorge, das Austesten, die Planung von Ausfallvorsorge etc. können von den immer weniger werdenden Beschäftigten mit Überblick kaum noch bewältigt werden. Die notwendige Zeit für die Überprüfung von Softwareveränderungen (jedes System enthält in unvermeidbarer Weise einen gewissen Prozentsatz an Fehlern – auch wenn dies Verschwörungstheorien zumeist anders deuten) fehlt zumeist, genauso wie die für System- und Integrationstests. Angesichts dessen ist es eher erstaunlich, dass es erst jetzt zu einem solch umfassenden Systemcrash gekommen ist. Im kleineren Rahmen von regionalen oder nationalen Firmenbereichen geschehen solche mehr oder weniger kleinen Katastrophen fast täglich, ohne dass davon viel in die Presse kommt (oder dann als „Softwarepanne“ kleingeredet wird).

Die hier aufgezeigte Entwicklung im IT-Bereich zeigt, dass sich sowohl in Bezug auf Sicherheit wie auf den lebenswichtigen Betrieb von IT-Systemen angesichts der globalen Konzentration derselben im bestehenden kapitalistischen System enorme Krisenpotentiale herausgebildet haben. Die Verwertungszwänge des großen IT-Kapitals führen zu enormem Arbeitsaufwand, um immer unsicherer werdende und komplexere Systeme noch betreiben zu können. Die Antwort kann nur sein, dass diese Großsysteme vergesellschaftet und unter Kontrolle der IT-Beschäftigten und die großer, selbstorganisierter, vernetzter IT-Communities gestellt werden, die sowohl den sicheren Betrieb lebenswichtiger Infrastruktur, die Datensicherheit und menschengerechte Arbeitsbedingungen für IT-Beschäftigte zur Priorität machen, statt immer höhere Umsätze und Profite für einige wenige IT-Mogule.