Facebooks Tsunami

Der Facebook-Ausfall und die ungeahnten Folgen

Wie kann ein gigantischer Internetdienst wie Facebook, der auf viele Standorte weltweit verteilt ist, innerhalb von Minuten von der Bildfläche verschwinden? Da muss einiges zusammenkommen – und das, was zusammenkam, taugt sehr gut als Lehrstück und Warnung für alle, die sich auf das Internet und ihr eigenes Können verlassen.

Von Dušan Živadinović

An einigen Nutzern ist Facebooks Ausfall am 4. Oktober 2021 unbemerkt vorübergegangen; er dauerte nur sechs Stunden. Doch für viele der 3,5 Milliarden Facebook-Nutzer waren das lange sechs Stunden mit teils ungeahnten Folgen.

Dabei verschwanden nacheinander innerhalb einer halben Stunde alle essenziellen Router und Server des Konzerns in der Versenkung und damit Facebooks soziales Netzwerk, die Webauftritte und die Dienste Messenger, WhatsApp und Instagram. Manche Netzwerkspezialisten vermuteten schnell, dass es sich um einen Konfigurationsfehler handeln musste und blieben gelassen (siehe ct.de/ygaw).

Aber für viele User, die sich anderswo im Internet ausschließlich über ihre Facebook-Zugangsdaten anmelden, waren viele von Facebook eigentlich unabhängige Internetdienste nicht erreichbar. Weltweit mussten Firmen, die mit Kunden normalerweise über Facebook kommunizieren, Einnahmeverluste hinnehmen.

Mark Zuckerberg, Gründer und Chef von Facebook, verlor nach Schätzungen des Nachrichtenmagazins Bloomberg 6 bis 7 Milliarden US-Dollar (5 bis 6 Milliarden Euro), als die Aktie seines Konzerns an den Börsen abstürzte. Danach war Zuckerberg nur noch 120 Milliarden Dollar schwer. Im Nachgang könnten Kunden wegen nicht ausgespielter Werbung ein Hühnchen mit Facebook rupfen wollen, vom Image-Verlust ganz zu schweigen.

Zudem hagelte es Spott und Schelte von Sicherheitsexperten. Beispielsweise unterlegte Steve Weis, Security-Spezialist und ehemaliger Facebook-Mitarbeiter, eine Visualisierung des etwa halbstündigen Abschaltvorgangs mit zappeligen Saxophonklängen des Songs Yakety Sax, mit der einst viele Benny-Hill-Sketche unterlegt wurden. Und Phillip Hallam-Baker, Kryptografiespezialist und Autor von Netzwerk-Spezifikationen twitterte süffisant: „Das ist ein Fehler, der ein sehr hohes Maß an Fachwissen erfordert“.

Manchen Mitbewerbern spülte der Ausfall Kunden zu. Viele Facebook-Nutzer haben ersatzweise zu anderen Kommunikationsmitteln gegriffen. Dokumentiert ist ein erheblicher Anstieg des SMS-Verkehrs und eine Zunahme an Usern, die etwa auf Messenger von Signal und Discord auswichen (siehe ct.de/ygaw).

Durch den Ausfall verloren Facebook-Mitarbeiter ihre Zugänge zu internen Tools, und zwar auch zu solchen, die sie zur Behebung solcher Probleme nutzen. Dazu gehören Facebooks interne E-Mail-Kommunikation und die Zugangsausweise der Mitarbeiter. Einige Berichte legen nahe, dass die Facebook-Zentrale handlungsunfähig war.

„Das ist ein Fehler, der ein sehr hohes Maß an Fachwissen erfordert.“

Kollateralschäden

Es gab auch Kollateralschäden. Cloudflare, der Betreiber des weltweiten Resolver-Dienstes, der unter der IP-Adresse 1.1.1.1 erreichbar ist, meldete einen Anstieg an DNS-Anfragen um das 30-Fache – die Erklärung liegt auf der Hand: Alle Internetdienste sind auf die Auflösung von Domainnamen zu IP-Adressen angewiesen, um mit Servern Kontakt aufzunehmen. Startet man Facebooks Messenger, fragt er den konfigurierten Resolver, unter welcher IP-Adresse der zugehörige Server angesprochen wird. Wenn er innerhalb einiger Sekunden keine Antwort bekommt, wiederholt er seine Anfrage. Je nach Programmierung kann das auch in immer kürzeren Intervallen passieren, was die Anfragefrequenz weiter erhöht, ebenso wie ungeduldige User, die ihre Apps immer wieder neu starten, in der Annahme, dass der Fehler im Smartphone sitzt.

Cloudflare gibt zwar an, die erhöhte Last gut weggesteckt und viele Anfragen trotzdem noch in vertretbarer Zeit beantwortet zu haben (max. 10 ms). Aber kleinere Resolver dürften unter der erhöhten Last eingeknickt sein, mit der Folge, dass sie DNS-Anfragen zu beliebigen Zielen nur noch langsam beantworten konnten.

Software-Patzer

Für Facebooks Reparaturmannschaft waren die Folgen schlimmer, denn auch die hauseigenen DNS-Server antworteten nicht mehr. Das stellte sie vor zusätzliche Probleme. Einige Admins waren laut der New York Times zur Reparatur zu einem Rechenzentrum im kalifornischen Santa Clara ausgerückt, um einen „manuellen Reset“ der Server zu versuchen. Sie kamen aber nicht mal in das Gebäude hinein – denn Facebook verwendet eine Internet-basierte Zugangskontrolle, die nur dann funktioniert, wenn die eigenen DNS-Server erreichbar sind.

Wie es letztlich gelang, den Fehler auszumerzen, wird Facebook vermutlich für sich behalten. Wichtiger erscheint aber die Beschreibung der Ursachen, denn die möchte jeder Firmen- und Heimnetz-Admin vermeiden.

Über den genauen Auslöser schweigt Facebook zwar. Man kann aber davon ausgehen, dass am Anfang ein Bedienfehler stand, ein fehlerhaftes Kommando in einem Konfigurationswerkzeug, mit dem

Netzbetreiber und große Inhalteanbieter Routen zu ihren Netzwerken gegenüber anderen Teilnetzen des Internet bedarfsgemäß annoncieren und zurückziehen (Border Gateway Protocol, BGP). Santosh Janardhan, Vice President für Infrastruktur bei Facebook, schreibt in einem Blog-Eintrag, dass man mit dem Befehl eigentlich nur die globale Backbone-Kapazität messen wollte.

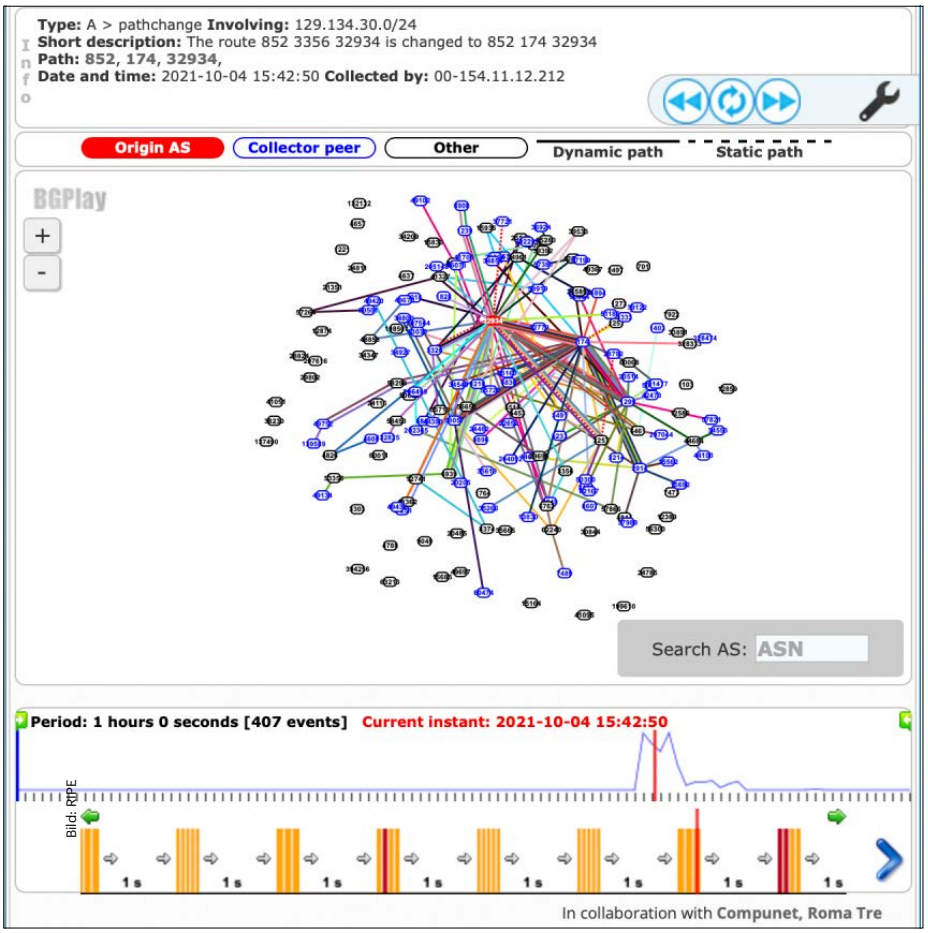
Stattdessen rutschte der Fehler im Kommando durch. Dann kam ein bis dahin offenbar nicht bekannter Fehler in einem Auditing-Tool hinzu: Dieses hätte den Bedienfehler erkennen und das verhängnisvolle Kommando stoppen müssen, ließ ihm aber freien Lauf. Facebook beschreibt die Folgen so: „Bei dem Ausfall wurde das gesamte Backbone-Netz von Facebook abgeschaltet. Daraufhin deklarierten sich alle Standorte selbst als defekt und zogen ihre BGP-Annoncen zurück."

Visualisiertes Verschwinden

Das dürfte der ersten halben Stunde entsprechen, während der nacheinander alle Routen zu Facebook-Servern und -Routern gelöscht wurden. Diesen Ablauf haben manche Netzwerkadmins mit Tools wie BGPlay der europäischen Netzverwaltung RIPE visualisiert, denn Vorgänge der BGP-Routenverwaltung protokollieren diverse Webdienste öffentlich. So ist auch optisch gut zu erkennen, wie der Befehl schrittweise alle Facebook-Annoncen getilgt hat.

Das Abschalten der Rechenzentren war schon Drama genug, aber hinzu kam ein Konzeptfehler: Anders als von Spezialisten empfohlen, setzt der Konzern zur Auflösung seiner eigenen Domains ausschließlich eigene DNS-Server und das auch nur im eigenen Netzwerk ein (autoritative DNS-Server). Diese sind so konfiguriert, dass auch sie ihre BGP-Annoncen zurückziehen, wenn die eigenen Rechenzentren nicht antworten. Das klingt nach einer Vorsorgemaßnahme gegen Attacken von außerhalb. Das Ergebnis war aber, dass kein Resolver der Welt DNS-Anfragen nach Facebook-Domains auflösen konnte; Facebooks autoritative DNS-Server, die den Resolvern die Informationen liefern sollten, fehlten jetzt.

Das verstärkte Facebooks Nöte, die Zusammenhänge überhaupt erst mal zu erkennen, weil auch Analyse- und Reparaturwerkzeuge auf eine funktionierende DNS-Auflösung angewiesen sind – ebenso wie die schon erwähnten Zugangskontrollsysteme. Facebook schildert das nur oberflächlich: „Das dauerte seine Zeit, denn diese Einrichtungen sind mit Blick auf hohe physische Sicherheit konzipiert. Es ist schwer, in sie einzudringen, und wenn man erst einmal drin ist, sind Server und Router so konzipiert, dass sie nur schwer verändert werden können."



Mit Online-Tools wie dem BGPlay der europäischen IP-Adressverwaltung RIPE lässt sich auch im Nachhinein visualisieren, wie Facebooks Server und Router schrittweise aus dem Internet verschwanden.

Heikle Reaktivierung

Man wüsste gern mehr zu diesem Vorgang, denn gemessen an der (wolkigen) Beschreibung des Sicherheitsniveaus erscheint ein sechsstündiger Ausfall eher kurz. Unterm Strich scheint Facebook glimpflich davongekommen zu sein. Das dürfte allerdings auch einer durchdachten Wiederaufnahme der Dienste geschuldet sein. Denn nachdem den Admins die Reaktivierung des Backbone-Netzwerks gelungen war, mussten die Rechenzentren wiederbelebt werden. Aber das ist ein heikler Akt: Laut Facebook nehmen nämlich manche der Rechenzentren im Normalbetrieb „mehrere zehn Megawatt" auf – doch beim gleichzeitigen Einschalten aller Komponenten könnte der Einschaltstrom die Hauptsicherung schmeißen. Dann können zum Beispiel Boot-Vorgänge scheitern und zu Fehlern auf Festplatten führen. Zumindest darauf war Facebook durch vorherige Stresstests vorbereitet und nahm den Betrieb nur schrittweise wieder auf.

Vier Tage später kam es jedoch erneut zu einem Ausfall, bei dem wieder mehrere Dienste des Konzerns betroffen waren. Diesen Ausfall behob Facebook innerhalb von zwei Stunden, nannte aber keine Gründe.

Immerhin verspricht Santosh Janardhan in einem Blog-Beitrag, dass der Konzern Lehren aus dem Vorfall ziehen werde. Von den meisten Änderungen wird zwar kaum etwas nach draußen dringen. Man wird aber sehen, ob die Firma es vielen anderen gleichtut und Backup-DNS-Server einrichtet (offsite secondary authoritative DNS). Anbieter gibt es genügend, auch für kleinere Firmen, siehe ct.de/-2643530. Andere Beispiele sind UltraDNS, Cloudflare oder GoDaddy. *(dz@ct.de)* c't

Visualisierung und Kommentare:
ct.de/ygaw