

Notfallstrategien für Trading-Unternehmen

Von Evgeny Sorokin



Notfallpläne für Situationen, die zum Ausfall des Online-Dienstes führen können, sind für Broker in besonderem Maße existenziell. Daher mahnt Evgeny Sorokin, für verschiedene Szenarien entsprechende Pläne vorzuziehen, sei es nun ein Cyberangriff oder auch „nur“ ein Stromausfall. Unterschätzt, so der Autor, sind dabei einfache Notfallplattformen, die im Notfall eine Zwischenlösung darstellen. Ergänzend können intelligente Bots für die Kundenkommunikation und als Ausweichmethode zum Versenden von Trading-Anweisungen zum Einsatz kommen. **Red.**

Jede Sekunde, in der Trading-Kunden nicht auf ihre Konten zugreifen können, fügt dem Image eines Brokers irreparablen Schaden zu und kostet eine Menge Geld. Deshalb benötigen Unternehmen einen Notfallplan mit präzisen Protokollen, der sofort einspringen kann – egal, wie schwerwiegend die Beeinträchtigungen sind.

Der Gedanke, sich gegen unvorhergesehene Ereignisse abzusichern, ist heutzutage fast allgegenwärtig. Es geht dabei nicht nur um die allgemeine Vorsorge, sondern vor allem darum, die bereits erzielten Fortschritte zu schützen. Das gilt besonders für Anbieter, die auf den Finanzmärkten aktiv sind. Sie stehen vor etlichen Hosting- und Backup-Herausforderungen und unterliegen sehr viel höheren Anforderungen, was die technische Verbindung zu Kunden und Liquiditätsprovidern betrifft. Zusätz-

lich macht die Funktionsweise der Finanzmärkte Ausfallzeiten äußerst problematisch: Steht das System still, lassen sich bei negativen Entwicklungen möglicherweise offene Positionen nicht schließen, ausstehende Orders nicht ändern und Trading-Algorithmen nicht abschalten.

Infrastruktur-Abhängigkeit vermeiden

Für alle unvorhersehbaren Ereignisse, die zum Ausfall des Online-Dienstes führen können, ist ein Notfallplan mit allgemeinen Wiederherstellungsstrategien existenziell. Hierzu gehören die routinemäßige Datensicherung auf einem ausgelagerten Speichersystem oder das externe Hosting einer Website-Kopie, die im Notfall einspringt.

Von Naturkatastrophen über interne Systemausfälle aufgrund von Hardware- oder Softwarefehlern bis hin zu Cyberangriffen oder einem Zusammenbruch der gesamten IT-Infrastruktur – auch wenn es sich bei diesen Vorstellungen meist um Worst-Case-Szenarien handelt, beginnt hier die Notfallplanung.

Oft lassen sich Unterbrechungen auf die Hosting- und Cloud-Anbieter zurückführen: Beispielsweise Ende 2021 betraf ein Ausfall von Amazon Web Services (AWS) diverse Universitäten, Unternehmen und Streaming-Dienste, die den Amazon-Cloud-Dienst nutzen. Grund dafür war vermutlich ein Stromausfall. Solche Fehler mahnen davor, sich nicht von einem einzelnen Infrastruktur-Anbieter abhängig zu machen.

Notfallpläne für verschiedene Krisenszenarien

Auch gezielte Angriffe von Hackern stellen ein großes Risiko dar: 2017 wurden die Datensätze von über 143 Millionen Kunden der größten US-amerikanischen Wirtschaftsauskunftei Equifax kompromittiert. Diese enthielten neben den Namen, Adressen und Sozialversicherungsnummern sogar Führerschein- und Kreditkartendaten.



Evgeny Sorokin, Senior Vice President of Software Engineering, Devexperts, München

Ein Unternehmen sollte daher mehrere individuelle Notfallpläne erstellen, um auf verschiedene Krisen optimal reagieren zu können.

– So erfordert ein Cybersecurity-Vorfall ein erstklassiges Sicherheitskonzept mit DDoS-Minderungsdiensten, die einen Hackerangriff automatisch abwehren und die interne IT-Infrastruktur festigen (DDoS steht für Denial-of-Services und stellt eine Dienstblockade dar).

– Ein Stromausfall hingegen verlangt nach einem Notstromgenerator. Je nach der Art und Größe des Unternehmens ergeben sich zudem individuelle Kriterien für den Notfallplan.

Die Herangehensweise muss aber in jedem Fall ganzheitlich ausgerichtet sein und alle wichtigen Ebenen der Firma einbeziehen: Netzwerk, Sicherheit, Server und Storage. Sämtliche Komponenten müssen dabei doppelt und vollsynchron repliziert werden.

Backup-Website und Stand-by-System

Ob etablierter Onlinebroker oder neuer Neobroker – wie krisenfest ein Notfallplan letzten Endes tatsächlich ist, liegt in der Regel im Können der Ingenieure, die sich um die Sicherheit und die IT des Unternehmens kümmern. Zudem werden Notfallstrategien und Best Practices oft erst eingeführt, nachdem sich ein kritischer Vorfall ereignet hat. Um jedoch im Voraus auf das Schlimmste gefasst zu sein, finden sich hier vier wichtige Notfallstrategien für Trading-Unternehmen:

Dazu gehört erstens, per Backup-Website den Geschäftsbetrieb zu sichern. Zum Schutz vor dem Worst-Case-Szenario (physische Gefährdung des Unternehmensstandorts) kann zweitens parallel zum Hauptsystem ein dediziertes Stand-by-System an einem anderen Ort eingerichtet werden. Auf diesem System laufen die Anwendungen des Brokers ebenfalls, allerdings im Read-only-Modus und ohne Kundenanforderungen zu verarbeiten. Erst wenn ein konkreter Notfall eintritt, übernimmt diese Stand-by-Umgebung aktiv und erhält die Anforderungen der Nutzer, wie etwa alle neu eingehenden Orders. Die Daten befinden sich auf

dem gleichen Stand, auf dem das Hauptsystem zum Zeitpunkt der Störung war.

Diese Maßnahme gewährleistet nicht nur die betriebliche Kontinuität, wenn es zu einer Katastrophe am Standort des Hauptsystems kommt. Auch bei Ausfällen wegen Wartungsarbeiten oder Reparaturen von Hard- oder Softwarefehlern lässt sich so der normale Betrieb sicherstellen. Die Aktualisierung der Systeme erfolgt bidirektional: Ist das Hauptsystem aktiv, wird das Stand-by-System aktualisiert. Arbeitet das Stand-by-System, wird das Hauptsystem auf Basis der neuen Daten des Stand-by-Systems aktualisiert.

Auf mehrere Liquiditätsprovider setzen

Viele Finanzdienstleister, insbesondere kleinere Firmen, können sich diese komplette Systemredundanz nicht leisten. Leider sind sie dadurch anfälliger für gravierende Störfälle wie Naturkatastrophen oder extreme Wetterlagen. Doch die Kosten der Implementierung und Wartung eines solchen Systems schießen oft abschreckend in die Höhe, da man praktisch die gesamte Trading-Infrastruktur an einem zweiten Standort nachbilden muss.

Um das Risiko zu verringern, dass ein Liquiditätsprovider Trades nicht akzeptiert oder die eingehenden Daten-Feeds veraltete Quotes beinhalten, gibt es zwei Lösungen: Zum einen können die Broker über einen Aggregator mit mehreren Liquiditäts Providern zusammenarbeiten. Zum anderen stehen ihnen professionelle Datenanbieter zur Verfügung, mit denen sie auch dann Kursdaten bereitstellen können, wenn Probleme bei einem oder mehreren Feeds auftreten. Diese Lösungen eignen sich natürlich nur bei Schwierigkeiten mit Liquiditäts Providern und nicht bei internen Hard- und Softwarefehlern, Netzwerkausfällen, DDoS-Angriffen oder anderen Bedrohungen der Cybersicherheit. Sie sind das absolute Minimum zum Schutz gegen den Katastrophenfall.

Einfache Sicherungsplattform für den Notfall einrichten

Unterschätzt, doch sehr effektiv, ist ein Kompromiss zwischen der vollständi-

gen externen Redundanz und gar keiner Ausfallsicherung: eine einfache Plattform, die nur in Notfällen zum Einsatz kommt. Sie ersetzt das vorhandene Brokersystem nicht, sondern stellt nur eine Zwischenlösung dar. Eine solche Plattform soll dem Kunden gestatten, auf seine Konten zuzugreifen und seine Positionen zu managen – oder es den Mitarbeitern ermöglichen, in seinem Auftrag zu handeln.

Sicherungsplattformen verhindern, dass das Brokergeschäft zum Erliegen kommt. Und was noch wichtiger ist: Während der Kunde darauf wartet, dass der Servicebetrieb wieder startet, kann er etwas tun. Jeder, der schon einmal den Ausfall seines Handelsplatzes erlebt hat, weiß, wie stressig diese Zeit sein kann; das gilt vor allem in einer Phase hoher Volatilität. Wer seine Trader so im Stich lässt, wird sie nicht halten können. Sie werden vermutlich zu Anbietern wechseln, die ihnen einen zuverlässigen Schutz gegen Systemausfälle bieten.

Einfache Notfallplattformen bestehen in der Regel aus einer abgespeckten Trading-Oberfläche, auf der sich die Kunden mit ihren Log-in-Daten anmelden können. Sie haben außerdem eine Schnittstelle zum letzten Back-up der Produktionsdatenbank, sodass die Kunden sämtliche Trading-Aktivitäten (zum Beispiel offene Positionen, ausstehende Orders oder ihre Social-Trading-Einstellungen) einsehen können. In der Regel sind Sicherungsplattformen nicht darauf ausgelegt, die volle Trading-Funktionalität bereitzustellen. Sie sollen lediglich die Möglichkeit eröffnen, offene Trades oder ausstehende Orders zu schließen, bis die Hauptplattform wieder läuft. Lösungen wie diese lassen sich auch als Backup bei einem „Deplatforming“ (Sperrung der Broker-Anwendung in den App Stores) einsetzen. So können die Kunden eine alternative, webbasierte Plattform nutzen, bis die Deplatforming-Entscheidung zurückgenommen wird.

Broker durch intelligente Bots unterstützen

Mit Assistenten wie einem intelligenten Bot steht den Brokern ein weiterer Kanal zur Kundenkommunikation zur Verfügung, der nicht nur effizient, sondern auch skalierbar ist. Er erweist sich für

das Notfallmanagement als ebenso hilfreich wie für die Bewältigung einer Flut von Anrufen, E-Mails und Live-Chats im Kundensupport.

Bei Störungen, die nicht direkt die Trading-Server eines Unternehmens betreffen, können Bots als Ausweichmethode zum Versenden von Trading-Anweisungen zum Einsatz kommen. Ähnlich wie bei der direkten telefonischen Übermittlung von Trades ermöglicht ein intelligenter Bot die Platzierung, Änderung oder Stornierung von Positionen und ausstehenden Orders über eine einfache SMS oder Sprachnachricht.

Sind keine Mitarbeiter an diesem Prozess beteiligt, können auch mehr Anfragen bearbeitet werden. Der Unterschied des Bots zum telefonischen Trading liegt nämlich darin, dass ein Bot direkt mit dem Trading-Server verbunden ist und weitaus mehr als nur eine einzige Anforderung auf einmal verarbeiten kann. So lassen sich menschlich bedingte Engpässe bei der Stornierung von Trades und ausstehende Orders vermeiden, wenn Webterminals, Webserver oder Datenzentren ausfallen oder angegriffen werden. Dasselbe gilt auch für Probleme mit Desktop-Plattformen oder wenn beispielsweise eine App aus einem iOS- oder Android-App-Store gelöscht wird. Entscheidend ist es, für jeden erdenklichen Notfall eine Lösung parat zu haben, die bei den Kunden Vertrauen schafft.

Jeder Broker versucht, wettbewerbsfähig zu bleiben, indem er auf Krisensituationen schnell reagiert. Leider geht dabei häufig etwas Porzellan zu Bruch, indem die Unternehmen beispielsweise ihren Marketingmaßnahmen den Vorrang vor der Produkt- oder Geschäftsentwicklung geben oder für aufsehenerregende Aktionen ihre Budgets überstrapazieren. Auch für Server-Auslastungsspitzen gibt es selten genug Spielraum, ganz zu schweigen von Ressourcen für das Notfallmanagement. Doch die Welt dreht sich immer schneller – niemand ist vor Ausfällen oder Angriffen hundertprozentig sicher. Die Cyberkriminalität entwickelt sich rasant und nimmt einen immer größeren Platz in unserem Alltag ein. Gute Gründe, spätestens jetzt intensiv über eine Notfallstrategie nachzudenken. ■