AUDIT MAGAZINE

ARTIKELEN | 1 JULI 2019

FINANCIAL CHAOS ENGINEERING

Auteur: Eric J.H.J. Mantelaers RA AA CISA CISO - Dr. Ing. Martijn M. Zoet
Beeld: Adobe Stock
Leestijd: 8 min

Maken uw bestuurders, net zoals de bestuurders van Pathé, 19 miljoen euro over wanneer ze daarover worden gebeld en gemaild door de accountant? Ofwel, wanneer een medewerker een e-mail van de baas krijgt, maakt hij dan het geld over? En hoeveel nepfacturen worden er door uw organisatie betaald.

Als het goed is komen de voorbeelden in het intro bij u niet voor. Maar werkt uw financiële systeem 100% foutloos? Dat is waarschijnlijk ook niet het geval. Er zijn altijd zaken die kunnen worden verbeterd. Veel managers en organisatieadviseurs beschouwen een organisatie te veel als een verzameling van bewust gemaakte en goed onderhouden afspraken.

Het zelfordeningsmechanisme uit de chaos- en complexiteitstheorie laat evenwel zien dat die veranderingen juist niet altijd kunnen worden beheerst, maar ‘vanzelf’ ontstaan en een eigen dynamiek hebben. Het is daarom belangrijk dat uw financiële systeem veerkracht toont en kan blijven functioneren. Het is wenselijk om een goed optimum te vinden tussen enerzijds de natuurlijke wil om een organisatie te beheersen en anderzijds de durf om een organisatie haar eigen dynamiek te laten hebben.

Toetsen van de veerkracht

Binnen informatie- en communicatietechnologie is er een discipline die de veerkracht van hard- en software toetst,

genaamd chaos engineering. Chaos engineering is door Netflix geïntroduceerd en als volgt gedefinieerd: ‘Chaos engineering is the discipline of experimenting on a distributed system in order to build confidence in the system’s capability to withstand turbulent conditions in production’.

Chaos engineering is door Netflix geïntroduceerd

In dit artikel introduceren wij het concept van financial chaos engineering, hetgeen we baseren op de principes zoals deze zijn gedefinieerd voor chaos engineering binnen het informatietechnologiedomein. Wij definiëren financial chaos engineering als volgt: ‘Financial chaos engineering is de discipline van experimenteren op het financieel systeem binnen de organisatie om vertrouwen te hebben dat het financiële systeem fraude en turbulente condities kan weerstaan tijdens dagelijkse werkzaamheden’.

In normaal Nederlands staat hier het opzettelijk doorbreken van onderdelen van de financiële systemen binnen de organisatie, zijnde de administratieve organisatie en de interne beheersing, zowel geautomatiseerd als niet-geautomatiseerd. Wanneer onderdelen van deze administratieve organisatie en/of de interne beheersing worden doorbroken, dan dient bepaald te worden wat er moet gebeuren, de impact dient gemeten te worden en de problemen dienen verholpen (gecorrigeerd) te worden, zodat de interne organisatie veerkrachtiger wordt voor de toekomst.

Experimenten op het financieel systeem

De gedachte om experimenten vanuit risk management, compliance en/of accountancy uit te voeren op het financieel systeem van een organisatie is relatief nieuw. Desondanks voeren organisaties al experimenten uit om onderdelen van de organisatie te toetsen. Een voorbeeld van een onderdeel dat vaker getoetst wordt, is de ICT-omgeving en met name de ICT-beveiliging. Een chaos monkey is een voorbeeld van zo’n experiment. Het verschil tussen de chaos monkey en de financial chaos monkey (FCM) is het gebied waarop de aanval wordt uitgevoerd. Bij de FCM is dit het financiële systeem van het bedrijf of de organisatie waarbinnen dit experiment wordt uitgevoerd. In het vervolg van dit artikel wordt de manier waarop financial chaos engineering geïmplementeerd kan worden nader toegelicht.

Implementatie financial chaos engineering

We onderkennen in het algemeen vier verschillende stappen bij de implementatie van financial chaos engineering:

1. Definieer de ‘steady state’ als een meetbare output hoe het systeem optimaal functioneert.
2. Definieer events (aanvallen) die het systeem van deze steady state kunnen afbrengen en definieer voor elk van deze aanvallen ook de risico’s.
3. Automatiseer de experimenten.
4. Voer de experimenten uit in de live-omgeving, maar minimaliseer de impact op de financiële huishouding.

Om de hiervoor genoemde vier stappen te concretiseren, beschrijven we deze inclusief een voorbeeld, namelijk een spookfactuur. Andere typen en complexere aanvallen zijn natuurlijk ook mogelijk. Hierbij kan onder andere gedacht worden aan: 1) het verzoek tot het (ongeoorloofd) muteren van een bankrekeningnummer, 2) het aanmelden van een nieuwe medewerker (deadman on the payroll), 3) een ‘besmette’ usb-stick aanleveren met een administratie van een klant, 4) aanvraag van een ongeoorloofde wijziging van een bankrekeningnummer van een klant, 5) het onterecht aanmaken van een creditfactuur.

1. ***Definieer de steady state als een meetbare output van het systeem dat een normaal gedrag definieert***
   In een normale organisatie is er sprake van een sluitende ‘three-way-match’, wat betekent dat de inkoopfactuur van bestelde en ontvangen onderdelen pas betaald mag worden nadat (in functiescheiding) is vastgesteld dat de bestelde hoeveelheid onderdelen correct ontvangen is en de bijbehorende inkoopfactuur juist is voor wat betreft: 1) het soort onderdelen, 2) de prijs ervan. Een voortdurend sluitende ‘three-way-match’ – waarvan een ‘correcte’ inkoopfactuur een belangrijk onderdeel is – is een weergave van de zogenaamde steady state.

2. ***Definieer events (aanvallen) die het systeem van deze steady state kunnen afbrengen en definieer voor elk van de aanvallen ook de risico's***
   Om de werking van de organisatie met betrekking tot de 'three-way-match' te toetsen, kunnen als aanval facturen worden ingebracht met onjuiste aantallen of onjuiste prijzen, zogenaamde spookfacturen. Om zoveel mogelijk aan te sluiten bij de werkelijkheid moeten dergelijke testfacturen op dezelfde wijze als de normale facturen (zoveel mogelijk geautomatiseerd) worden ingevoerd in het systeem. Mochten deze spookfacturen er overigens doorheen glippen, dan is op deze testfactuur een 'eigen' bankrekeningnummer vermeld, zodat het geld niet verloren gaat.
   Omdat deze beschrijving voor een specifieke aanval te vaag is, kan er gebruikgemaakt worden van een template om een concrete aanval te definieren. Deze template bestaat uit zeven onderdelen, namelijk: a. doelwit, b. experimenttype, c. hypothesen, d. 'blast radius', e. status vóór aanval, f. status na aanval en g. bevindingen van de aanval.

Als de administratieve organisatie en interne beheersing niet naar behoren functioneren, dan wordt uiteindelijk de spookfactuur ten onrechte betaalbaar gesteld en betaald

a. *doelwit*
Het doelwit van een aanval kan alle essentiële en vitale onderdelen van een financiële organisatie betreffen. In het geval van de spookfactuur betreft het doelwit de werking (het functioneren) van de inkooporganisatie en in het bijzonder de crediteurenadministratie.

b. *experimenttype*
Het experimenttype deelt de experimenten op in vooraf gedefinieerde categorieën. Echter, omdat er vooralsnog geen standaardstructuur bestaat, beschrijven we hier geen specifiek voorbeeld.

c. *hypothesen*
Het 'inschieten' van een spookfactuur is zoals beschreven een vereenvoudigd voorbeeld van financial chaos engineering. Op basis hiervan kunnen twee (H0 en H1) hypothesen worden geformuleerd.
H0 – de spookfactuur krijgt een factuurnummer toegekend, wordt het proces ingeschoten en wordt geblokkeerd door de controleur van de inkooporganisatie die de prijzen, hoeveelheden, kwaliteiten en dergelijke moet controleren.
H1 – de spookfactuur krijgt een factuurnummer toegekend, wordt het proces ingeschoten en wordt uiteindelijk onterecht betaald.

d. *blast radius*
Onder blast radius wordt verstaan de impact die een aanval op de organisatie kan hebben. Hierbij wordt gestreefd naar een zo groot mogelijke impact, waarbij de organisatie zo min mogelijke schade wordt toegebracht. Hoever reiken de gevolgen van deze spookfactuur? Als de in de interne organisatie opgenomen administratieve organisatie en interne beheersing (AO/IB) niet naar behoren functioneren, dan wordt uiteindelijk de spookfactuur ten onrechte betaalbaar gesteld en betaald. Geld verlaat de organisatie zonder dat er een tegenprestatie tegenover staat. Daaraan voorafgaand wordt natuurlijk de inkooporganisatie (crediteurenadministratie) geraakt, waardoor de werking van dit deel van de AO/IB ter discussie komt te staan. De werking van de AO/IB is primair van belang voor het bedrijf zelf. De leiding van dit bedrijf streeft immers een betrouwbare informatievoorziening na.

e. *status vóór aanval*
Bij de status vóór aanval wordt beschreven hoe de organisatie functioneert voordat de aanval heeft plaatsgevonden. De verantwoordelijke leiding van het bedrijf waarbinnen de FCM wordt toegepast, heeft de interne organisatie zodanig opgebouwd dat de gewenste taken worden uitgevoerd, rekening houdend met de vereiste

controletechnische functiescheidingen. Dit betekent bijvoorbeeld dat iemand die onderdelen bewaart (magazijn) niet de bevoegdheid heeft om te beschikken over de bankrekening en dus de inkoopfactuur niet kan betalen. Door een adequate inrichting (opzet) van de AO/IB en een constant functioneren hiervan (bestaan en werking) mag de leiding erop vertrouwen dat de taken correct worden uitgevoerd en de processen naar behoren functioneren, waardoor de informatievoorziening ook adequaat zal functioneren.
Concreet is dit voor de leiding van het bedrijf de basis om erop te vertrouwen dat betaalde inkoopfacturen hebben geleid tot de ontvangst van bestelde onderdelen die aan de eisen voldoen. De accountant die namens het toezichthoudend orgaan of de leiding van het bedrijf wordt ingeschakeld voor de controle van de jaarrekening zal – afhankelijk van zijn controleaanpak – waar mogelijk willen steunen op en gebruikmaken van de in de interne organisatie opgenomen AO/IB. Als we kijken naar de eerdergenoemde hypothesen, lijkt het geoorloofd dat de accountant in geval van H0 steunt op die interne organisatie.

f. *status na aanval*
Bij de status na aanval wordt beschreven hoe de organisatie functioneert nadat de aanval heeft plaatsgevonden. In geval van H1 is de spooknota ten onrechte betaald en heeft geld (zonder tegenprestatie) de organisatie verlaten. Het vertrouwen in bepaalde medewerkers en dus in de werking van de AO/IB (inlooporganisatie en de crediteurenadministratie) is geschaad. Wanneer de accountant na verloop van tijd constateert dat zijn vertrouwen wordt geschaad omdat H1 van toepassing is en gebleken is dat de vermeende adequate AO/IB niet naar behoren functioneert, dan zal hij zijn controle-aanpak moeten wijzigen. Of, nog erger, zal hij zijn opdrachtcontinuering moeten heroverwegen. Immers, de integriteit van de leiding staat mogelijk ter discussie.

g. *bevindingen*
Bij de sectie bevindingen wordt zodra de aanval is afgerond, beschreven wat de eventuele gevolgen zijn voor de opzet, het bestaan en de werking van de interne organisatie. Deze gevolgen dienen te worden geëvalueerd en omgezet te worden in acties, die vervolgens geffectueerd dienen te worden. Indien de aanval met goed gevolg is afgeweerd, dan wordt dit ook hier geconstateerd en gedocumenteerd.

3. ***Automatiseer de experimenten***
   Om de aanvallen met minimale inspanning en herhaalbaar te kunnen uitvoeren, dienen zij zoveel mogelijk te worden geautomatiseerd. In ons voorbeeld kan een server elke maand een of meerdere spookfacturen inschieten. Belangrijk is dat het beheer van deze server onder verantwoordelijkheid staat van de allerhoogste bedrijfsleiding.

4. ***Voer de experimenten uit in de live-omgeving maar minimaliseer de impact op de financiële huishouding***
   De organisatie is erbij gebaat de experimenten zo waarheidsgetrouw mogelijk uit te voeren. Daarom dienen experimenten in een live-omgeving plaats te vinden. In sommige gevallen zal dit niet mogelijk zijn. Bijvoorbeeld bij een aanval met een flash-crash of een beurscrash, omdat de aanval dan mogelijk een grote schade toebrengt aan de organisatie. Dergelijke aanvallen kunnen dan beter worden gesimuleerd.

Three lines of defense

In het kader van de interne beheersing onderkent men binnen organisaties de zogenaamde first, second en third line of defense. De eerste lijn betreft de proceseigenaren. De tweede lijn zijn de mensen die verantwoordelijk zijn voor compliance of risk management. De derde lijn betreft de interne accountantsdienst. Normaliter zullen de mensen in de first line vooraf niet op de hoogte zijn van financial chaos engineering, al zullen ze na verloop van tijd wel bekend zijn met het fenomeen spookfacturen en het feit dat deze kunnen opduiken. Dit zou een preventieve werking kunnen hebben. Afhankelijk van de omvang van het bedrijf en de diverse afdelingen, kunnen zowel de tweede als de derde lijn betrokken zijn bij het voorbereiden van bewuste chaosacties. De interne accountantsdienst zal gebruikmaken van de bevindingen

van deze acties.

Afhankelijk van de omvang van het bedrijf en de diverse afdelingen, kunnen zowel de tweede als de derde lijn betrokken zijn bij het voorbereiden van bewuste chaosacties

Traditioneel gezien maken accountants uit het oogpunt van efficiency (waar mogelijk) gebruik van de AO/IB die aanwezig is in de interne organisatie. In dit kader voeren deze accountants een interimcontrole en een eindejaarscontrole uit. Tijdens deze laatste controle wordt normaliter de balans 'dichtgevinkt', terwijl tijdens de interimcontrole de opzet, het bestaan en de werking van de organisatie wordt getoetst. In het licht van de beoordeling van de betrouwbaarheid van de informatievoorziening hebben zowel de leiding van het bedrijf (intern) als ook de externe accountant (extern) gelijke belangen. Normaliter wordt vastgesteld of de organisatie werkt zoals die zou moeten werken. Het is daarbij (nog) niet gebruikelijk om de organisatie 'voor de gek te houden' en te kijken of men (door of namens de accountant) gemaakte fouten eruit weet te halen.

Over
Eric Mantelaers is hoofd Bureau Vaktechniek en auditpartner bij RSM Nederland Accountants nv, docent accountantsopleiding Maastricht University, lid van het lectoraat van Zuyd Hogeschool 'Optimaliseren Kennisintensieve Bedrijfsprocessen' en PhD fellow Open Universiteit.

Martijn Zoet is als lector verbonden aan het lectoraat van Zuyd Hogeschool 'Optimaliseren Kennisintensieve Bedrijfsprocessen'. Tevens is hij als managing partner verbonden aan EDM-Competence Centre.

De auteurs hebben dit artikel geschreven op persoonlijke titel.

Tags: cyber security, informatiebeveiliging

Bron url: https://auditmagazine.nl/artikelen/financial-chaos-engineering/