

Downtime is money

Ghid practic pentru a afla cat downtime isi poate permite afacerea ta

1. Introducere
2. Cati bani pierzi la downtime ?
3. Cati bani aloci ca sa te protejezi ?
4. Cum distribui bugetul eficient ?

1. Introducere

Bogdan Belu - www.bogdanbelu.ro

- 16 ani experienta tehnica si de business in administrare de sistem, programare si servicii datacenter
- din 2001 director general la Distinct (www.distinct.ro), furnizor de managed services si datacenter sub sloganul “plus prin responsabilitate”
- clienti reprezentativi Distinct: TAROM, Libertatea, Europa FM, Capital, Evenimentul Zilei, TVR

Definirea problemei

- subiectul: impactul si prevenirea downtime-ului solutiilor IT
- depindem de tehnologie atat noi cat si afacerile noastre
- suntem afectati semnificativ cand tehnologia nu functioneaza cum trebuie
- pentru o afacere, pierderile se pot cuantifica in bani si acestea se pot minimiza prin aplicarea unei strategii

De ce discutam acest subiect ?

- sunt prea putini responsabili de proiect care isi pun problema "what if ?" inainte sa fie prinsi nepregatiti de un downtime
- in general, se aplica zicala "tot patitu-i priceput", cred ca este mai bine sa invatam din experienta altora
- presiunea pe bugete este in continuare mare si tendinta este sa se taie din planificare si prevenirea riscurilor
- pentru ca avem de fiecare data discutia "de ce e asa scump ?" cu managerii de proiect

Termeni

- **Downtime:** perioada de timp in care sistemul nu indeplineste parametri minimi de utilizare (nu-si atinge scopul principal)
- **Downtime partial:** doar anumite aspecte ale sistemului nu functioneaza (ex: adaugarea/inregistrarea de noi utilizatori)
- Termenul opus este: **Uptime** (cat timp sistemul este in regula), se exprima % de functionare pe an:

Uptime/an	Downtime/an
0%	8760 h
90%	876 h
95%	438 h
99%	87h, 36m
99.9%	8h, 45m, 36s
99.99%	52m, 33s
99.999%	5m 15s
99.9999%	31 s

2. Cati bani pierzi in caz de downtime ?

- ideal ar fi sa faci un exercitiu de imaginatie, inainte sa se intample, pentru a estima pierderile cauzate de un astfel de eveniment
- ca sa faci o evaluare ai nevoie de sa-ti cunosti bine cel putin:
 - a) structura cheltuielilor si procesele de business
 - b) dinamica tranzactiilor pe intervale orare din saptamana (exemplu: posibil ca sambata noaptea la ora 3 sa nu pierzi la fel de multi bani ca vineri la ora 11)
 - c) sezonalitatea (exemplu: o promotie anuntata la TV, luna decembrie pentru comercianti, inceputul verii pentru furnizorii de aer conditionat)
 - d) impactul duratei problemei (in general impactul tinde sa se accentueze pe masura ce durata creste)

Exemplu

Premise:

- magazin online care vinde legume/fructe bio
- site-ul este lansat de un an
- vanzarile medii zilnice sunt de 1000 EUR/zi
- comanda medie este de 25 EUR
- are in medie 40 de clienti/zi
- distributia incasarilor: 10% profit, 25% costuri fixe (regie si promovare), 65% costuri pe tranzactie (furnizori, transport)
- un client fidel face o achizitie pe saptamana, exista aproximativ 250 de clienti fideli (returning customers)
- in primele 12 luni s-au cheltuit pe promovare 30000 EUR (120 EUR/returning customer)
- vinerea, numarul de clienti si vanzarile sunt duble (2000 EUR/zi)
- in septembrie, sezon de conserve, valoarea unei achizitii este dubla (50 EUR)
- 70% din vanzari se intampla in timpul saptamanii (Luni-Vineri, 10-18), 30% din vanzari se fac seara si in weeked

Downtime si impact

Downtime:

- Downtime: site-ul nu este functional timp de 6 ore din cauza suprasolicitarii bazei de date, in luna septembrie, vineri, intre orele 10-16

Impact:

- vanzarile din ziua respectiva scad cu 50% (-2000 EUR din CA anual)
- din 80 de clienti potentiali in ziua respectiva, 40 se decid sa cumpere de la supermarket sau de la concurenta
- 5 clienti fideli decid sa se mute permanent la concurenta, se pierd 30 de achizitii din viitor pentru fiecare client (-3750 EUR din CA anual)
- este chemat de urgenta un expert sa rezolve problema (+250 EUR cheltuieli)
- moralul echipei: suprasolicitarea pe nervii tai si ai angajatilor necesita o iesire cu echipa in oras (+100 EUR la cheltuieli)
- 1 client face review negativ pertinent pe un forum de profil (-500 EUR din CA)
- livrarile comandate cu o zi inainte nu au ajuns la timp pentru ca interfata backoffice a site-ului nu a fost functionala, un client fidel este pierdut (-750 EUR din CA anual)

Analiza

Rezumat:

- downtime de 6h intr-o zi importanta
- incasarile scad cu 7000 EUR dar cheltuielile scad doar cu 4550 EUR (cost marfa la furnizori, transport), diferenta: 2450 EUR
- cheltuielile ocazionale cresc cu 350 EUR
- impact per total: pierderi de 2800 EUR (0.77% din CA)

In concluzie:

- In general cheltuielile tind sa scada semnificativ mai putin decat incasarile
 - Procesul de analiza nu este simplu dar trebuie facut la nivelul de detaliu pe care il permite business-ul (sa nu coste procesul in sine mai mult decat potentialele pierderi)
 - Analiza trebuie facuta periodic precum si la fiecare noua adaugare de elemente de infrastructura
- Nota: sunt pierderi care nu pot fi cuantificate in bani (in general cele legate de viata, aparare nationala, sanatate)

3. Cati bani aloci ca sa te protejezi ?

- odata ce ai datele din simulare, cel mai sigur este sa pasezi riscul partial sau total la fiecare din specialistii implicati in crearea si intretinerea sistemului prin solicitarea unui SLA (Service Level Agreement)
- specialistii (programatori, administratori de sistem, datacenter, content manageri) cunosc cel mai bine probabilitatea unui anumit eveniment nedorit si pot calcula costurile de prevenire, interventie si rezolvare
- fiecare dintre acestia iti va da un pret pe SLA-ul cerut; in functie de bugetul disponibil si apetitul de risc poti ajusta cerintele pentru a obtine un cost final
- dormi mai linistit noaptea si te poti concentra pe core business
- ca regula generala: costurile tind sa creasca cu un ordin de marime cu fiecare 9 adaugat dupa virgula la cifra de uptime (exemplu: 1 EUR pt. 99%, 10 EUR pentru 99.9%, 100 EUR pentru 99.99%)
- cand ai pierderi potentiale ce nu pot fi cuantificate in bani (ex: legate de sanatate) aloci maximum de buget disponibil

Exemplu de SLA

In timpul orelor de program (Luni-Vineri 10-18):

- timp de interventie maximum: 2h
- timp de rezolvare functionalitate principala a sistemului: 2h (de la interventie)

In afara orelor de program:

- timp de interventie maximum: 6h
- timp de rezolvare functionalitate principala a sistemului: 4h

Daca SLA-ul nu este respectat se vor acorda despagubiri de: 100 EUR pentru fiecare ora de nerespectare

Nota: clauza de rezolvare se acorda de obicei pe probleme clar identificate

Furnizorii specializati calculeaza riscurile si costurile

Furnizorul sau furnizorii vor calcula riscul de producere al evenimentelor si costurile pentru a le preveni sau a interveni/rezolva in timpul cerut:

Exemple de elemente luate in considerare:

- HDD-uri in RAID, surse de alimentare redundante
- mentinerea unui sistem identic in standby gata sa-l inlocuiasca pe cel principal
- generator de curent cu pornire automata in cazul in care se intrerupe alimentarea cu energie electrica
- prezenta pieselor de schimb on-site
- administrator de sistem in standby
- programator oncall care sa poata interveni de la distanta
- mecanisme de rezerva in cazul in care un om nu este disponibil (bolnav, concediu, nu are semnal la telefon)

Sugestii

- atunci cand este posibil, este bine sa lucrezi cu cat mai putini furnizori pentru ca pot oferi un SLA unic pe mai multe elemente (exemplu: datacenter + administrare de sistem)
- de preferat, colaboreaza cu furnizori suficient de mari (pot acoperi mai usor problemele in afara orelor de program, au mecanisme de rezerva pentru oameni si echipamente mai bine puse la punct)
- relatiile cu furnizorii trebuie sa fie pe termen lung (interventiile vor fi mai rapide si costurile mai mici daca este bine familiarizat cu sistemul)
- in general despagubirile din SLA trebuie sa fie legate de valoarea contractului cu furnizorul (nu poti sa ceri despagubiri de 10000 EUR la un contract de 500 EUR chiar daca tu pierzi suma asta)

4. Cum distribui bugetul cat mai eficient ?

- nu este economic fezabil sa acoperi 100% din cazuri, trebuie facuta o prioritizare pe principalele amenintari
- prioritizarea trebuie facuta de specialisti (Furnizori)
- chiar daca pasezi riscul catre Furnizori via SLA este bine sa te asiguri ca:
 - a) sunt acoperite intai cazurile de downtime permanent prin data loss (backup-uri, backup-uri incrementale, procedura de recovery testata)
 - b) SLA-ul pe datacenter este acoperitor si sunt prevazute cazurile de cedari hardware (piese de schimb, elemente redundante)
 - c) exista un sistem de monitorizare automat al infrastructurii si al aplicatiei:
 - se afla de o problema imediat ce apare
 - se alerteaza partile interesate imediat
 - se poate masura indeplinirea SLA-ului
 - d) acoperi si cazurile de probleme la nivel de aplicatie (programator si administrator de sistem)

- e) se invata din greseli
- f) ai la cine apela cand se intampla ceva neprevazut si te afecteaza in acel moment
- g) infrastructura si incidentele sunt documentate (knowledge base, tichete)
- h) schimbarile la sistem sunt dezvoltate si testate pe o infrastructura separata
- i) standardele general acceptate in domeniu sunt respectate (face mai usoara schimbarea responsabililor si interoperabilitatea)
- j) in proiecte mari, nu lasa evaluarea/planificarea sa fie ingroapata sub un munte de birocratie
- k) securitatea informatica este tratata cu seriozitate

Concluzii

- 1) aloca resurse planificarii initiale
- 2) este important sa stii cat te poate afecta un downtime inainte sa se intample, cel mai bine cuantifici in bani
- 3) paseaza sau imparte riscul cu furnizorii specializati folosind un SLA clar
- 4) stabileste costurile si termenii SLA-ului pe baza feedback-ului furnizorilor, a bugetului maxim disponibil si a apetitului la risc
- 5) asigura-te ca lucrezi cu furnizori de incredere

Incheiere

- Aceasta prezentare o gasiti si online la www.bogdanbelu.ro
- Va astept la stand-ul Distinct daca doriti sa discutam mai multe pe acest subiect
- Q&A