

Recuperarea datelor în caz de dezastru

Crezi că ai totul sub control? Mai gândește-te!

Nicio companie nu e imună la dezastre care au potențialul de a cauza întreruperea sistemelor IT. Momentele în care sistemele IT nu funcționează (downtime-ul IT) pentru perioade lungi îți pot lăsa compania fără acces la date și echipamente critice pentru activități esențiale.

Și, în timp ce echipa IT încearcă să rezolve problema, compania ta poate suferi din cauza pierderii productivității, având totodată un impact negativ asupra relației cu publicul și reputației companiei tale. În timp ce multe companii cred că sunt pregătite pentru toate tipurile de scenarii de dezastru, există altele care nu sunt pregătite deloc.



1 Ai deja un plan de recuperare a datelor în caz de dezastru?

73%

Numărul de companii mici și mijlocii din Marea Britanie care nu au în vigoare niciun plan de continuitate.

75%

Numărul de companii mari care nu au în vigoare niciun plan de continuitate.

Companiile acordă o importanță mai mare sau mai mică planului de recuperare a datelor în caz de dezastru (DR/Disaster Recovery), de obicei având următoarele motive:

- Cred că nu li se poate întâmpla lor.
- Nu vor să investească într-un plan DR de care nu este nevoie 99.9% din timp.
- Au folosit benzi magnetice pentru backup de ani de zile și nu cred că este nevoie de o schimbare.



Știi că?

Gartner prezice că costul mediu al unui downtime IT este de aprox. £4,400 pe minut.

2 Crima cibernetică este motivul care duce cel mai des la căderea sistemelor IT în companiile din Marea Britanie



Rapoartele prezic că atacurile cibernetice vor costa economia mondială £4.5 miliarde pe an până în 2021.



În 2017 s-au înregistrat 184 de milioane de atacuri ransomware la nivel mondial.



Companiile din Marea Britanie sunt supuse atacurilor ransomware de 38 de ori pe zi.

Mediu de afaceri riscant

Pe lângă crima cibernetică, există o mulțime de alte amenințări potențiale cu care companiile se pot confrunta oricând:



În 2017 British Airways a suferit o întrerupere majoră a serviciilor IT care a dus la o mulțime de zboruri anulate și la clienți nemulțumiți.



Aceasta a fost și cauza întreruperii serviciilor Visa în 2018 care a lăsat milioane de companii din Marea Britanie fără posibilitatea de a procesa plăți cu cardul de credit.



Un angajat al Amazon Web Services (AWS) Simple Storage Service (S3) a provocat în mod involuntar o întrerupere care a cauzat probleme unora dintre cele mai populare website-uri ale lor, inclusiv Netflix și Spotify.



Deși Marea Britanie stă mult mai bine în comparație cu alte părți ale lumii în ceea ce privește daunele provocate din cauza furtunilor și a inundațiilor, anul trecut zeci de mii de case și companii au suferit întreruperi ale energiei electrice din cauza furtunii Eleanor.

3 Este planul tău de DR conceput astfel încât să ți se potrivească?

Doar minimul de downtime al sistemelor tale IT critice este acceptabil pentru a i se întâmpla companiei tale, pentru restul este timpul să acorzi atenție planurilor de recuperare a datelor în caz de dezastru (DR).

- 1 Ai testat planul tău actual DR și aceasta a funcționat corespunzător?
- 2 Sunt serviciile și datele tale critice protejate în cel mai eficient mod?
- 3 Crezi că infrastructura ta DR este adecvată companiei tale sau investiția este cea corespunzătoare?
- 4 Ce plan există dacă în acest moment sistemele tale primare ar cădea?
- 5 Crezi că organizația ta ar avea de beneficiat de pe urma serviciilor DR bazate pe cloud?

4 Ai opta pentru Recuperarea Datelor în Caz de Dezastru ca Serviciu (DRaaS)?

DRaaS ia de pe umerii Managerului IT orice ține de recuperarea datelor în caz de dezastru, oferindu-i acestuia liniștea de care are nevoie știind că toate sistemele critice ale companiei sunt protejate, securizate și complet recuperabile. Acest serviciu oferă:

- Copierea și găzduirea atât fizic cât și virtual în cloud a serverului de către un terț furnizor pentru a asigura reluare automată în caz de nereușită.
- Duplică infrastructura, aplicațiile și datele din mai multe locații în cloud, permițând ca toate acestea să fie complet recuperabile.
- Sunt disponibile opțiuni flexibile de recuperare a datelor, așa cum sunt restaurarea aplicațiilor unice sau a întregii infrastructuri.



Dacă vrei să fii sigur că datele tale critice sunt protejate în cazul unui dezastru, atunci vizitează [website-ul nostru](#) sau apelează +4 031 080 0700 pentru a vorbi cu unul dintre experții noștri.

+4 031 080 0700
sales@m247.ro

Surse

Companii mici și mijlocii/Companii mari
<https://www.tandemsystems.co.uk/blog/2015/10/07/73-of-uk-smes-lack-a-disaster-recovery-plan>
Eroare umană
<https://www.information-age.com/human-error-growing-preventable-123465498/Storm>
<https://www.information-age.com/ten-biggest-business-continuity-disasters-cost-uk-businesses-billions-123461455/>
Atacuri Ransomware
<https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/>
<https://www.telegraph.co.uk/technology/2018/03/10/british-businesses-battle-38-ransomware-attacks-day/>
Întreruperea energiei electrice la British Airways
<https://www.theguardian.com/business/2017/may/31/ba-it-shutdown-caused-by-uncontrolled-return-of-power-after-outage>

Visa
<https://www.computerweekly.com/news/252442416/Visa-blames-hardware-failure-for-UK-wide-card-payment-system-outage>
Furtună
<https://www.independent.co.uk/news/uk/home-news/storm-eleanor-live-updates-latest-news-uk-weather-winds-rain-flooding-power-cuts-homes-travel-roads-a8139111.html>
Costul unui downtime
<https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/>