BACKUP AND RECOVERY STRATEGIES AND THEIR ROLE IN BUSINESS CONTINUITY

STRATEGII DE BACKUP ȘI RECUPERARE ȘI ROLUL LOR ÎN CONTINUITATEA AFACERII

Zgureanu Aureliu
Doctor în științe fizico-matematice, conferențiar universitar
Academia de Studii Economice a Moldovei
e-mail: zgureanu.aureliu@ase.md

Abstract
IT disaster recovery is one of the most important component of business continuity process. Companies need it for recovering disrupted systems and networks and resume normal operations every time when disruptions occure. Disaster recovery becomes more important from day to day because it allows minimizing any negative impacts to company operations. Disaster recovery is a business continuity process that ensures access to the software, hardware, and data required to resume normal business operations in the event of a natural or human-induced disaster. Implementation of a good distaer recovery plan begins with choosing the best strategies for this goal. The correlation of the business continuity, disaster recovery and the best strategies in this field are analysed in this paper.

Keywords: *backup, recovery, disaster, business continuity, strategy.*

JEL Classification: *H12, M15*

INTRODUCERE

În IT, un dezastru poate fi orice problemă neașteptată care duce la o încetinire, întrerupere sau o eroare într-un sistem cheie sau o rețea. Aceste probleme pot fi cauzate de dezastre naturale (adică incendii, cutremure, uragan, etc.), erori tehnologice, acte rău intenționate, diverse tipuri de incompatibilități sau chiar de simple erori umane. Probabilitatea ca un astfel de dezastru să aibă loc poate crește odată cu dezvoltarea organizației și a infrastructurii sale IT, a concurenței neloiale și a multor altor factori. Totodată, cea mai bună apărare orientată spre evitarea urmărilor dezastruoase ce pot apărea în astfel de situații constă în planificarea continuității afacerii și a recuperării datelor în caz de dezastru, folosind cele mai bune practici și strategii care ghidează organizațiile în prevenirea și/sau gestionarea mai bună a evenimentelor perturbatoare imprevizibile.

Ținând cont de ultimele date statistice, o organizație nu poate să-și permită riscul confruntării cu un dezastru IT fără a fi pregătită de astfel de scenarii, deoarece urmările perturbărilor catastrofale ale datelor organizației, și implicit a reputației sale, o poate costa foarte mult, până chiar și la pierderea afacerii. Institutul Ponemon și IBM Security în raportul *Cost of a Data Breach Report* pentru anul 2020 [1] a constatat că costul mediu al unei încălcări de date la nivel global este de 3,86 milioane de dolari (3,90 în 2019 și 3,86 în 2018). Același raport pentru anul 2018 arată că 65 la sută dintre clienții cărora le-au fost compromise datele au spus că și-au pierdut încrederea într-o organizație, iar unul din trei a ales să-și întrerupă relația cu organizația afectată. În acest context recuperarea datelor capătă o conotație specială și devine una dintre elementele de bază ale Managementului continuității unei afaceri.

Standardul ISO/IEC 27031:2011: Tehnologia informației - Tehnici de securitate - *Linii directoare pentru disponibilitatea tehnologiilor de informare și comunicare pentru continuitatea afacerilor* specifică recuperarea dezastrelor IT ca capacitatea elementelor

TIC ale unei organizații de a-și susține funcțiile critice de afaceri la un nivel acceptabil într-o perioadă de timp prestabilită după o întrerupere. În același document este definit și Planul de continuitate a afacerii (BCP -Business Continuity Plan) și Planul de recuperare în caz de dezastru TIC (ICT DRP – Disaster Recovery Plan) [2].

Planul de continuitate a afacerii reprezintă un set de proceduri documentate care ghidează organizațiile să răspundă, să recupereze, să reia și să restabilească la un nivel predefinit de funcționare în urma întreruperii. În mod normal, aceasta acoperă resursele, serviciile și activitățile necesare pentru a asigura continuitatea funcțiilor critice ale afacerii.

Planul de recuperare în caz de dezastru TIC este un plan clar definit și documentat care recuperează capacitățile TIC atunci când apare o perturbare (uneori acesta se mai numește plan de continuitate TIC).

Astfel, recuperarea resurselor IT în caz de dezastru este un set standard de politici și proceduri pe care o afacere sau o organizație le pune în aplicare și le urmează pentru a se proteja pe sine și personalul său în fața unui dezastru. Planurile de recuperare în caz de dezastru pot ajuta compania să asigure securitatea angajaților, a hardware-ului și software-ului, restaurarea sistemelor și a elementelor conexe continuității afacerii. DRP-urile pot include măsuri preventive, măsuri corective și măsuri detective pentru a preveni cât mai mult posibil dezastrele care ar putea afecta întreprinderile, reducând în același timp, într-un mod cât mai fiabil posibil, impactul unui dezastru.

Măsurile preventive sunt acele măsuri care diminuează riscul și previn apariția unui dezastru IT, iar exemplele de aceste măsuri includ backup-ul datelor în cloud, efectuarea de audituri de securitate de rutină etc. Măsurile detective ajută la descoperirea potențialelor amenințări, de exemplu, actualizarea software-ului antivirus, instalarea software-ului de monitorizare server/rețea etc. Măsurile corective conțin pașii necesari pentru restabilirea rapidă a sistemelor IT lovite de dezastru. Toate aceste măsuri sunt importante în realizarea procesului de recupearre IT și deaceea trebuie tratate cu responsabilitate maximă.

CONTINUITATEA AFACERILOR

Continuitatea afacerii (BC - Business Continuity) este procesul de minimizare a riscului de perturbare. Mai precis, continuitatea afacerii înseamnă efortul necesar pentru a reduce probabilitatea unui incident perturbator și pregătirea organizației pentru a continua livrarea celor mai esențiale produse și servicii, dacă ar avea loc o perturbare.

Un proces de continuitate a afacerii ar trebui să implice la două lucruri:

- înțelegerea riscurilor legate de perturbările cu care se poate confrunta afacerea;
- încrederea executivilor în capacitatea organizației de a reacționa și de a se recupera.

Acesta poate fi numit nivelul corect de reziliență. Continuitatea afacerii este, de asemenea, cunoscută sub numele de planificare a continuității, reziliență organizațională sau management al continuității afacerii.

Continuitatea afacerii se bazează pe parcurgerea a câtorva pași fundamentali [3]:

a) în primul rând, este necesar de a identifica produsele sau serviciile critice care trebuie protejate;
b) apoi, trebuie identificate riscurile pentru produsele sau serviciile respective; acestea sunt cel mai adesea resursele necesare livrării, în special persoane, tehnologii, facilități, echipamente și terțe părți;
c) odată ce resursele sunt identificate, este necesar de a implementa strategii care protejează resursele cheie (cum ar fi munca la distanță, procesele manuale sau facilități alternative);
d) în continuare, pot fi documentate planurile de continuitate a afacerii care prezintă modul de implementare a strategiilor de recuperare;

e) în cele din urmă, se efectuează exerciții și teste pentru a confirma că planurile și strategiile funcționează conform așteptărilor.

Există o serie de discipline legate de continuitatea afacerii, inclusiv:

- *managementul situațiilor de urgență* - este o disciplină axată pe probleme specifice instalației care implică siguranța vieții și protecția proprietății;
- *recuperarea în caz de dezastru*, cunoscută și sub numele de *recuperare în caz de dezastru IT* - este o disciplină axată pe protejarea și recuperarea tehnologiei și a datelor;
- *managementul riscului* - continuitatea afacerii este un tip special de proces de management al riscului; alte procese de gestionare a riscurilor includ conformitatea și securitatea informațiilor;
- *managementul crizelor* - acest efort se concentrează pe răspunsul executiv la perturbări și este o parte cheie a continuității afacerii.
- *comunicarea în situații de criză* - acest efort se concentrează pe aspectul de comunicare când reacționăm la un dezastru și merge mână în mână cu gestionarea crizelor.

De ce am avea nevoie de conceptul „continuitate a afacerii”? Continuitatea afacerii ajută la protejarea unei organizații, indiferent de dezastrul care poate apărea. Și acest lucru este important în lumea din ce în ce mai imprevizibilă de astăzi! Fie că este vorba de perioade de nefuncționare neprogramate ale tehnologiei, de o întrerupere a lanțului de aprovizionare, de un dezastru natural sau de un eveniment provocat de om, organizațiile de toate dimensiunile recunosc că trebuie să fie pregătite pentru aproape orice. Majoritatea organizațiilor construiesc un plan de continuitate a afacerii din unul dintre cele trei motive:

- clienții o cer (cel mai frecvent în modelul B2B);
- autoritățile de reglementare o cer (cel mai frecvent în domeniul bancar și energetic);
- consiliul de administrație sau directorii superiori o cer (recunoscând responsabilitatea lor fiduciară).

Toate aceste grupuri solicită continuitatea afacerii ca o modalitate de a proteja organizația pe termen lung.

Continuitatea afacerii este reglementată la nivel internațional de standardul ISO 22301, care la nivel național este înscris în registrul de Stat al standardelor sub numele „SM EN ISO 22301:2020. *Securitate și stabilitate. Sisteme de management al continuității activității. Cerințe*” [2]. Există patru beneficii esențiale ale afacerii pe care o companie le poate obține prin implementarea acestuia:

1. Respectarea cerințele legale. Există din ce în ce mai multe țări care definesc legi și reglementări care necesită respectarea continuității afacerii. Și dincolo de interesele guvernamentale, întreprinderile private (de exemplu, instituțiile financiare) solicită, de asemenea, furnizorilor și partenerilor să implementeze soluții de continuitate a afacerii. Și vestea bună este că ISO 22301 oferă un cadru și o metodologie perfectă pentru a sprijini respectarea acestor cerințe - prin reducerea efortului administrativ și operațional, precum și a penalităților care trebuie plătite.

2. Obținerea unui avantaj de marketing. Dacă o companie este certificată ISO 22301 și concurenții ei nu, respectiva companie va avea un avantaj față de aceștia atunci când vine vorba de clienții care sunt sensibili la păstrarea continuității operațiunilor lor și la livrarea produselor și serviciilor lor. În plus, o astfel de certificare poate ajuta și la obținerea de clienți noi, facilitând demonstrarea apartenenței la cei mai buni din industrie, ceea ce duce la creșterea cotei de piață și la profituri mai mari.

3. Reducerea dependenței de peronal. De cele mai multe ori, activitățile critice ale unei companii se bazează doar pe câțiva oameni greu de înlocuit - situație demonstrată dureros când acești oameni părăsesc organizația. Directorii care sunt conștienți de acest lucru pot face uz de practicile de continuitate a afacerii pentru a deveni mult mai puțin

dependenți de acei angajați ai săi (fie datorită soluțiilor implementate pentru o eventuală înlocuire a acestora, fie prin documentarea sarcinilor conexe), ceea ce înseamnă că se poate preveni o mare durere de cap atunci când cineva părăsește organizația.

4. Prevenirea daunelor la scară largă. Într-o lume a serviciilor și tranzacțiilor în timp real, fiecare minut de stagnare costă bani - mulți bani. Și, chiar dacă afacerea nu este atât de sensibilă la perioade mici de indisponibilitate, incidentele perturbatoare o vor costa. Prin implementarea practicilor de continuitate a activității conforme ISO 22301 se obține un fel de poliță de asigurare. Fie prin prevenirea incidentelor perturbatoare, fie prin capabilitatea de recuperare mai rapidă - compania va economisi bani. Și, cel mai bun lucru dintre toate este că investiția în ISO 22301 este mult mai mică decât economiile pe care le va realiza compania.

RECUPERAREA DATELOR ÎN CAZ DE DEZASTRU

După cum am menționat mai sus – una dintre discipline legate de continuitatea afacerii este *recuperarea în caz de dezastru* – cunoscută și sub numele de recuperare în caz de dezastru IT.

Secțiunea A.17 din anexa A la ISO/IEC 27001 are ca obiectiv pentru o organizație încorporarea continuității securității informațiilor în sistemele sale de gestionare a continuității activității. Pentru a susține acest lucru, această secțiune oferă controale legate de procedurile de continuitate a afacerii, planuri de recuperare și redundanțe [5].

Cu toate acestea, la fel ca toate standardele sistemului de management, ISO 27001 descrie doar ceea ce trebuie realizat, însă nu și cum. Nici ISO/IEC 27002 - colecția de bune practici pentru ISO 27001- nu ajută prea mult în acest sens [8].

Însă familia ISO/IEC 27000 are standarde suplimentare care vizează domenii specifice, iar unul dintre ele este ISO/IEC 27031, care acoperă disponibilitatea tehnologiei informației și comunicațiilor pentru continuitatea afacerii (sau IRBC - ICT Readiness for Business Continuity) și ne ghidează cu privire la ce trebuie să luăm în considerare atunci când dezvoltăm continuitatea afacerii pentru IT - de obicei, aceasta se numește „recuperare în caz de dezastru”. Implementarea ISO/IEC 27031 devine tot mai actuală odată ce tot mai multe activități ale companiilor moderne au devenit dependente de tehnologiile informației și comunicațiilor, iar erorile și defecțiunile IT devin din ce în ce mai critice.

În acest context, standardul ISO/IEC 27031 abordează modul de utilizare a ciclului PDCA (Plan-Do-Check-Act) pentru a pune în aplicare un proces sistematic de prevenire, prezicere și gestionare a incidentelor de perturbare a serviciilor TIC sau a celor care au potențialul de a perturba aceste servicii [3]. Procedând astfel, acest standard ajută la susținerea atât a managementului continuității afacerii, cât și a managementului securității informațiilor. Prin natura sa, ISO/IEC 27031 este un standard perfect pentru realizarea controlului A.17.2.1 din ISO/IEC 27001 (disponibilitatea mijloacelor de prelucrare a informației) [5].

Este adevărat că termenul de recuperare în caz de dezastru nu este un termen oficial ISO și, în consecință, sensul său nu este universal acceptat. Cu toate acestea, majoritatea profesioniștilor IT identifică acest termen cu capacitatea de a recupera infrastructura IT în caz de perturbare. Prin urmare, ISO 27031 este cel mai potrivit dintre standardele ISO anume în acest scop.

Este necesar aici de precizat unele diferențe esențiale între ISO 27031 și ISO 22301. În primul rând, ISO 22301 acoperă continuitatea afacerii în ansamblu, considerând orice tip de incident ca o sursă potențială de perturbare (de exemplu, boală pandemică, criză economică, dezastru natural etc.) și utilizând planuri, politici și proceduri pentru a preveni, reacționa, și recupera după perturbările cauzate de acestea. Aceste planuri, politici

și proceduri pot fi clasificate în două tipuri principale: cele pentru continuarea operațiunilor, dacă afacerea este afectată de un eveniment de perturbare și cele pentru recuperarea infrastructurii IT, în cazul în care sunt perturbate tehnologiile IT.

Prin urmare, ne putem gândi la ISO 27031 ca la un instrument pentru implementarea părții tehnice a ISO 22301, oferind îndrumări detaliate cu privire la modul de a face față continuității elementelor TIC pentru a ne asigura că procesele organizației vor oferi clienților rezultatele așteptate [2]-[3].

ISO 27031 recomandă șase categorii principale care necesită a fi luate în considerare la planificarea continuității afacerii cu referință la elementele care implică TIC și care pot răspunde la întrebările principale care apar în procesul de asigurare a continuității [2]:

1. *Abilități și cunoștințe*: strategiile de recuperare includ luarea în considerare a abilităților tehnice specializate și a cunoștințelor necesare pentru a opera serviciile IT până la, în timpul și după o perturbare; strategiile care includ considerări privind abilitățile și cunoștințele se concentrează pe asigurarea faptului că niciun individ nu deține abilități sau cunoștințe specializate care ar fi necesare pentru a opera sistemele IT ale organizației.
   Aici trebuie luate în considerare:
   - informațiile care sunt necesare pentru a rula serviciile IT critice;
   - persoanele care dețin aceste informații;
   - modul în care pot fi încorporate aceste informații în cunoștințele organizaționale și puse la dispoziție cu ușurință;
   - modul în care organizația face disponibile aceste informații în caz de dezastru.
2. *Echipamente*: strategiile de recuperare includ reducerea riscului asociat cu operarea sistemelor TIC bazate pe un singur echipament; strategiile care includ considerări privind echipamentele asigură utilizarea sistemelor IT chiar dacă echipamentul primar devine inoperabil.
   Pentru aceasta este necesar de avut în vedere:
   - condițiile care ar trebui să le respecte dispozitivele și infrastructura pentru a minimiza riscurile de perturbare sau timpul de recuperare;
   - locul unde ar trebui amplasate astfel de facilități.
3. *Tehnologia*: strategiile de recuperare includ luarea în considerare a cerințelor tehnice necesare pentru a îndeplini cerințele de recuperare ale organizației, în special Obiectivul Timpului de Recuperare (RTO) și Obiectivul Punctului de Recuperare (RPO); strategiile mai includ considerări tehnologice care implică asigurarea faptului că hardware-ul și software-ul și datele pot fi recuperate în timpul solicitat de organizație.
   Aceste considerări ar trebui să includă:
   - tehnologiile cele mai importante pentru afacere - sisteme de asistență, cum ar fi alimentarea, răcirea, personalul, asistența furnizorului și conectivitatea WAN;
   - cerințele de recuperare, de exemplu, RTO, RPO, dependența de alte tehnologii, etc.
4. *Date*: strategiile de recuperare includ luarea în considerare a modului de protejare a datelor solicitate de organizație.
   Strategiile privind datele includ:
   - securitatea, validitatea și disponibilitatea datelor solicitate de utilizatorii finali;

- datele necesare pentru a restabili activitățile comerciale și în ce perioadă de timp (de reținut că RTO și RPO pentru serviciile IT sunt diferite de RPO și RTO pentru date);
- controalele de securitate (de exemplu, controlul accesului) care trebuie să existe în permanență pentru a securiza datele.

5. *Procese*: strategiile de recuperare includ luarea în considerare a modului de susținere a proceselor necesare pentru a monitoriza, opera și recupera sistemele IT pentru a satisface cerințele afacerii; strategiile care iau în considerare procesele identifică procesele IT necesare înainte, în timpul și după o întrerupere a sistemelor IT și anume:
   - procesele pe care le avem la dispoziție pentru a face față unui incident sau dezastru;
   - modul în care procesele necesare pentru a crea elemente din categoriile 1-4 funcționează împreună pentru a furniza serviciile comerciale necesare (de exemplu, comunicații, aplicații, acces utilizator etc.).
6. *Furnizori*: strategiile de recuperare includ luarea în considerare a modului de informare și implicare a furnizorilor care sunt necesari pentru recuperarea și operarea sistemelor TIC.

   Aceste strategii definesc:
   - furnizorii implicați în operarea și recuperarea sistemelor TIC înainte, în timpul și după ce a avut loc o întrerupere;
   - consumabilele (de exemplu, copii de software și piese de schimb hardware) esențiale pentru continuitatea IT, modul în care se pot asigura furnizorii companiei că pot susține cerințele de continuitate a afacerii acestei companii.

STRATEGII DE BACKUP ȘI RECUPERARE

Backup-ul este procesul de creare a unei copii a datelor din sistemul ce trebuie protejat. Această copie se utilizează pentru recuperare în cazul în care datele originale ale organizației sunt pierdute sau corupte. De asemenea, putem utiliza o copie de rezervă pentru a recupera copii ale fișierelor mai vechi, dacă ele au fost șterse din sistem. Multe companii și organizații își protejează datele critice cu ajutorul copiilor de rezervă, făcându-le una dintre componentele cheie ale planului de recuperare în caz de dezastru și ale strategiei de continuitate a afacerii.

Recuperarea este foarte importantă pentru companii, deoarece ele sunt foarte dependente de date. La fel cum o persoană nu poate supraviețui fără aer, apă și alimente, întreprinderile nu pot supraviețui fără date. În conformitate cu raportul anual al phoenixNAP pentru anul 2020 [4], 40-60% dintre întreprinderile mici care pierd accesul la sistemele operaționale și la date fără un plan de recuperare în caz de dezastru își pierd afacerea pentru totdeauna, iar companiile care se pot recupera fac acest lucru la un cost mult mai mare și la un interval de timp mai extins decât companiile care aveau un plan clar de backup și recuperare în caz de dezastru. În același timp 96% dintre companiile care au implementată o soluție de recuperare în caz de dezastru și-au recuperat complet operațiunile.

Odată cu creșterea atacurilor malware și a creșterii costului unei încălcări a securității datelor, securitatea cibernetică a devenit o prioritate de afaceri. Cu toate acestea, chiar și cu măsuri de securitate înăsprite, încălcările au crescut cu 67% în ultimii 5 ani. Drept urmare, nevoia de a avea o strategie solidă de backup a devenit mai importantă ca niciodată. Pentru a fi cu adevărat protejate, organizațiile trebuie să formeze un plan bine definit, care să ajute la recuperarea rapidă și fără probleme a datelor pierdute și să garanteze continuitatea afacerii atunci când toate măsurile preventive eșuează.

O strategie cuprinzătoare pentru recuperare este o parte esențială a conceptului de securitate cibernetică a unei organizații. Ea poate fi definită ca un plan al administratorului pentru a se asigura că datele organizaționale critice sunt copiate și disponibile pentru restaurare în cazul unei situații de pierdere a datelor. O strategie de backup, împreună cu un plan de recuperare în caz de dezastru, constituie unul dintre pilonii de bază în continuitatea afacerii și poate ajuta o organizație să reziste unui atac cibernetic și să se recupereze cu daune minime sau chiar nule pentru afacere, reputație și date.

Abordările care vin să stabilească o strategie în acest sens pot fi diferite de la companie la companie, însă acestea pot fi generalizate prin patru pași, necesari pentru dezvoltarea unei strategii solide de backup, propuși de Matt McDermott, directorul de management al produselor (inclusiv backup-ul) pentru Office 365 și anume [6]:

1. *Determinarea datelor care trebuie copiate*. Pornind de la ideea că toate datele ar trebui să fie copiate, nivelul de protecție a datelor ar varia în funcție de cât de important este să recuperăm un set de date sau altul. Obiectivul timpului de recuperare (RTO) al organizației, care reprezintă *durata maximă acceptabilă necesară pentru ca o organizație să recupereze datele pierdute și să revină la funcționalitatea acceptabilă*, ar constitui un punct de referință fiabil atunci când ne formăm strategia de backup. Este recomandat ca aplicațiile și datele se fie evaluate și grupate în:
   - existențial-critice pentru ca afacerea să supraviețuiască;
   - critice pentru ca organizația să funcționeze;
   - optime pentru performanță pentru ca organizația să prospere;

   Odată identificate toate datele pertinente, este necesar de a acoperi nivelul de protecție corespunzător.
2. *Determinarea frecvenței cu care trebuie făcută o copie de rezervă a datelor*. Frecvența cu care facem o copie de rezervă a datelor companiei ar trebui să fie aliniată cu obiectivul punctului de recuperare (RPO) al organizației, care este definit ca *perioada maximă admisibilă între momentul pierderii datelor și ultima copie de rezervă utilă a unei stări bune cunoscute*. Astfel, cu cât datele sunt salvate mai des, cu atât este mai probabil să respectăm RPO-ul declarat al acestei organizații. Ca regulă generală, copiile de backup trebuie efectuate cel puțin o dată la 24 de ore pentru a îndeplini standardele acceptabile ale majorității organizațiilor.
3. *Identificarea și implementarea unei soluții adecvate de backup și recuperare*. Pe baza cerințelor organizației trebuie de identificat o soluție de backup adecvată ca parte a strategiei de backup. Iată câteva aspecte de luat în considerare la identificarea soluției de backup și recuperare:
   - tipurile de backup: backup complet, backup diferențial (în care sunt copiate numai adăugările/modificările) și backup incremental (în care se modifică diferența de la cel mai recent backup incremental);
   - unde se va păstra backup-ul: backup fizic/local (în care datele sunt copiate la fața locului utilizând un hard disk extern, o unitate USB, etc.) sau backup cloud/remote (unde datele sunt salvate în afara locației într-un mediu de stocare cloud);
   - caracteristici necesare organizației: ușurința de realizare a backup-ului (opțiuni automatizate și/sau la cerere), restabilirea flexibilității (între utilizatori, bazat pe căutare, punctual), scalabilitatea (gestionarea licențelor și utilizatorilor), ușurința de utilizare (o interfață utilizator intuitivă și recuperarea self-service), experiența după cumpărare (asistența gratuită și spațiu de stocare nelimitat), recomandări solide (evaluări pozitive ale clienților, certificări de securitate și conformitate).
4. *Testarea și monitorizarea sistemului.* Odată ce sistemul backup este instalat, el trebuie testat, atât pentru a verifica dacă atât backup-ul, cât și restaurarea au fost realizate cu

succes. Trebuie de verificat backup-ul și restaurarea referitor la diferite tipuri de artefacte – conturi, e-mailuri, documente, site-uri etc. Dacă soluția de backup acceptă backup-ul utilizatorului final – este necesar de a informa și educa utilizatorii despre modul de folosire a acestuia. La fel este important să fie monitorizată performanța copierii de rezervă și să fie verificate în mod regulat jurnalele referitor la pierderea de date.

Aici trebuie de mai menționat regula frecvent menționată când vine vorba de backup-ul datelor, și anume strategia (sau regula) 3-2-1, care este utilizată ca protocol de bază și la care se mai adaugă alte caracteristici pentru a se asigura un nivel optim de securitate. Această regulă include:

- asigurarea că avem 3 copii ale datelor;
- stocarea copiilor pe 2 dispozitive separate;
- păstrarea unei copii într-o locație la distanță.

În ultimul timp devine actuală și versiunea 3-2-2 a acestei reguli, în care ultimul punct se completează cu 2 copii în loc de una, păstrate în locații diferite – una pe un server sau hard drive și alta în cloud. Această strategie ar trebui să ne protejeze împotriva erorilor software și hardware, hackerilor ransomware și a virușilor. Mai mult, această regulă ne poate proteja datele și în fața oricăror dezastre naturale.

Pentru a realiza o strategie fiabilă de recuperare în caz de dezastru subliniem (cu riscul de a ne repeta) câteva dintre aspecte prioritare ale celor mai bune practici în dezvoltarea acesteia:

costul - vom avea nevoie de un plan de backup a datelor pe care ni-l putem permite, pentru aceasta trebuie să analizăm cheltuielile potențiale ale unei încălcări sau pierderi, apoi, să cântărim acest lucru în raport cu costul proiectat al sistemului nostru de backup;

locul de stocare a copiilor de date - unele companii preferă backup-ul bazat pe cloud, altora le place să aibă o copie de rezervă fizică; cele mai prudente companii folosesc mai multe surse de rezervă, în acest fel, dacă o copie de rezervă eșuează, compania are o altă copie la dispoziție;

stabilirea riscurilor cu care ne putem confrunta referitor de date - fiecare companie trebuie să se gândească la riscurile provocate de malware și eventualele atacuri de phishing; cu toate acestea, este posibil ca acestea să nu fie singurele riscuri cu care compania se poate confrunta, spre exemplu o companie dintr-o zonă predispusă la inundații trebuie să ia în considerare daunele cauzate de apă; ar fi înțelept de asemenea să existe o soluție pentru backup și recuperare a datelor situată în afara locației companiei;

periodicitatea copierii de rezervă a datelor - unele companii generează date foarte frecvent, în astfel de cazuri, o copie de rezervă zilnică poate să nu fie suficientă, și este posibil să fie nevoie de un orar special pentru copiile de rezervă; pentru alte companii ale căror date sunt rar actualizate, o copie de rezervă o dată pe săptămână poate fi suficientă;

persoanele responsabile pentru planificarea backup-ului - instruirea angajaților este esențială pentru o strategie eficientă de backup. Este necesar ca în companie să exise personal cu cunoștințe solide în domeniu, pe care să ne putem baza la implementarea strategiei de backup și recuperare.

CONCLUZII

Continuitatea afacerii este „capacitatea strategică și tactică a organizației de a planifica și răspunde la incidente și perturbări ale afacerii pentru a continua operațiunile comerciale la un nivel predefinit acceptabil” [7], în timp ce recuperarea în caz de dezastru constă din „procesul, politicile și procedurile legate de pregătirea pentru recuperarea sau

continuarea infrastructurii tehnologice esențiale pentru o organizație după un dezastru natural sau indus de om".

După cum putem vedea din aceste definiții, accentul în recuperarea în caz de dezastru este pus pe tehnologie, în timp ce în continuitatea afacerii - este pus pe operațiuni de afaceri. Prin urmare, recuperarea în caz de dezastru face parte din continuitatea afacerii și am putea să o considerăm ca unul dintre principalii factori ai operațiunilor de afaceri sau ca parte tehnologică a continuității afacerii.

În fianl, cea mai importantă parte a evitarii intreruperii afacerii în cazul unui dezastru este planificarea timpurie. Prin stabilirea unor strategii fiabile de continuitate a afacerii și a recuperării în caz de dezastru, compania poate fi pregatită pentru o recuperare rapidă și eficientă, în cazul în care se declanșează un dezastru. Aceste strategii trebuie să includă obligator teste periodice pentru fi asigurați că planul se actualizează și pentru a putea evidenția eventualele vulnerabilități. Compania trebuie să fie pregatită să facă schimbări și să ofere instruire și resurse angajaților acolo unde este necesar, astfel încât în orice moment să fie sigură că planurile ei funcționează.

Indiferent de mărimea afacerii sau de experiența pe piata, toate organizatiile ar trebui să implementeze un plan de continuitate a afacerii și de recuperare în caz de dezastru și să le utilizeze împreună, pentru a asigura cea mai mare protecție împotriva întreruperii activității.

BIBLIOGRAFIE

1. IBM Security. *Cost of a Data Breach Report 2020*. Available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/.
2. SM ISO/CEI 27031:2013. *Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity.*
3. SM EN ISO 22301:2020. *Security and resilience. Business continuity management systems. Requirements*.
4. *2020 Disaster Recovery Statistics That Will Shock Business Owners*. Available at: https://phoenixnap.com/blog/disaster-recovery-statisticss.
5. SM EN ISO/IEC 27001:2017. *Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Cerinţe*.
6. Mcdermott, M. *Forming a Backup Strategy: 4 Steps to Follow*. Available at: https://spanning.com/blog/backup-strategy-4-steps-to-follow/.
7. BS 25999-2:2007. *Business continuity management. Specification*.
8. SM EN ISO/IEC 27002:2017. *Tehnologia informaţiei. Tehnici de securitate. Cod de bună practică pentru managementul securităţii informaţiei.*