Protejarea datelor prin backup

- **Întamplarea unu....**

În 1997, când a avut prima dată acces la un PC, domnul Calculătorescu şi-a făcut o lucrare importantă pe acesta, pe vremea aceea un frumos şi nou 486. Mare, greoi, dar era totuşi un PC şi mai ales nu era 286 (primul PC.. 286.. nu iau în calcul calculatoarele bazate pe microprocesorul Z80). Era o minunăție şi foarte scump: cam 1.000 $ pe vremea când salariul era cam de 150 $. A cumpărat o carte, în care scria că hard-disk-ul are spațiu limitat, (512MB în 1997) și că ar fi bine să mai treacă din datele salvate pe HDD, pe alte suporturi. Folosea pe vremea aceea, dischete de 5 inch. A luat tot ce a lucrat, a comprimat într-o arhivă, a pus arhiva împărțită pe patru dischete (ştia de arhivare multi-volum şi vechiul arj). Prima dischetă s-a stricat, a doua nu putea funcționa fără prima. In concluzie, toate datele pierdute. Si terminase cu lucrarea, făcuse totul. Era vorba de mai puțin de 5 MB de date, ceva absolut infim (la capacitatile vehiculate din ziua de azi). Nu a câștigat mare spațiu pe hard-disk... Cam1%... Dar a zis că lucrarea e protejata şi în caz de virusare. Munca a două luni de zile nu a fost pierdută, nu a fost inutilă, a fost ştearsa cu bună ştiinţă fără posibilitate de recuperare pentru că a crezut că o pusese în siguraţă pe disketele respective...

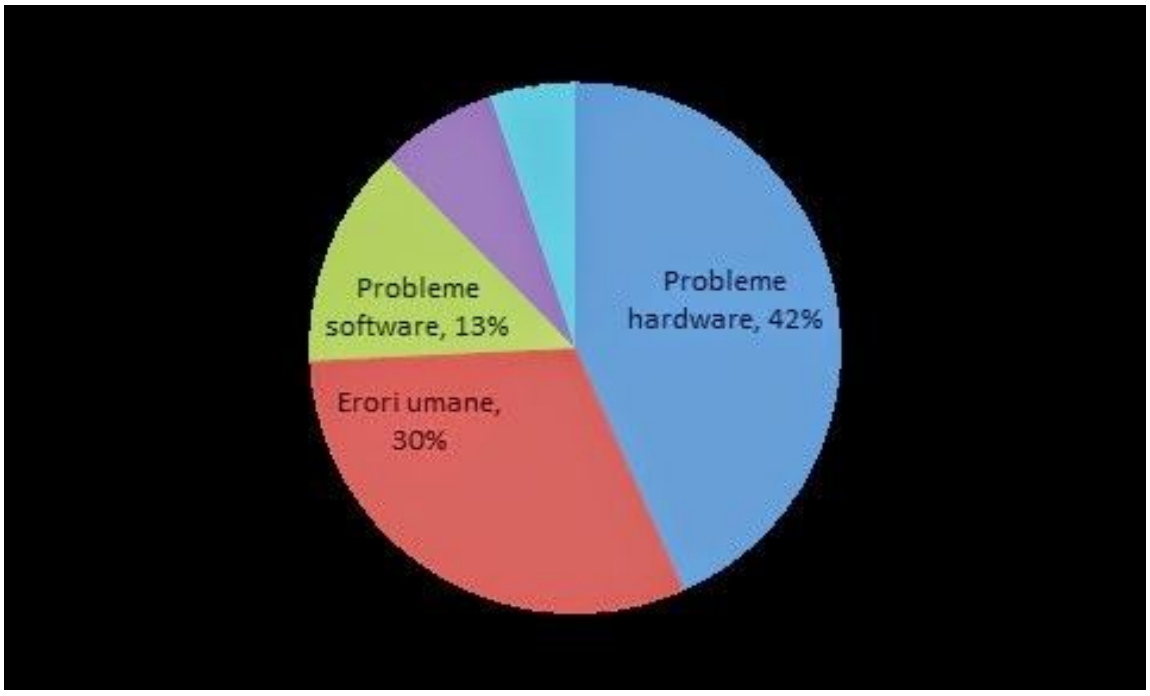
- **Întamplarea doi....**

Domnul Hărnicescu la un moment dat redacta într-un un serviciu o lucrare importantă. A lucrat o oră, a sunat telefonul, o altă problemă mai importantă.... A trebuit să abandoneze şi să închidă programul în care lucrase. A omis să salveze înainte lucrarea. Ce să vezi : a pierdut tot. Dupa rezolvarea celeilalte probleme urgente, a luat-o de la capăt. Lucrează intens şi concentrat. Iar suna telefonul, iar închide lucrarea, ...Aaaarhh!... He, he... Nu apăruse încă suita Office cu al său procesor de texte Word şi nici măcar Windowsul cu Wordpad inclus... Programele din ziua de azi te întreabă dacă salvezi şi dacă nu, oricum o fac ele din timp în timp preventiv şi-i pune lucrării un nume generic. Domnul Hărnicescu în 1997 lucra în MS Dos cu nişte programe rudimentare de editoare de text ai căror programatori încă nu se gândiseră cât de inventivi sunt utilizatorii în toate privintele şi sub toate aspectele....

- **Întamplarea trei....**

Să ne imaginam că, într-o dimineață, toate datele institutiei – e-mailuri, documente, bazele de date, liste de contacte, catalogări – dispar, din cauza unei situații care a apărut şi-a lăsat amprenta şi nu a fost prevăzută. Acest lucru este un coşmar dar se poate întâmpla din cauza unei defecțiuni hardware, a unui bug software sau datele pot fi șterse accidental sau mod intenționat de un membru sau un fost membru al instituţiei.

Aceste întâmplări au personaje şi nume imaginare pentru a nu leza pe cineva, dar sunt întâmplări din viaţa reală care pot fi cuprinse într-o imagine care arată că datele pot fi supuse foarte uşor deteriorării pe parcursul drumului străbătut între introducere - prelucrare - stocare din multiple cauze: erori umane în exploatare, greşeli umane în software şi în hardware. Problemele software pot fi de mai multe feluri: intentionate, (virusi, mallware) sau neintentionate, (defecte ale sistemelor de operare, ale programelor de prelucrare sau de stocare a datelor sau manipulari greşite ale acestora)



Lumea virtuala este expusă la multiple vulnerabilităţi ale datelor dacă acestea nu sunt securizate corespunzator. Back-up-ul datelor a devenit o procedură absolut necesară indiferent dacă există un singur utilizator de computer (laptop, tableta, telefon inteligent) sau membrii unei întregi

companii care procesează un volum foarte mare de informaţii**.**

O metoda esenţială pentru protejarea datelor, împotriva deteriorărilor sau a ştergerii lor este Backup-ul.

În majoritatea cazurilor, backup-ul este văzut ca un centru generator de costuri fără profit. Orice instituţie trebuie să aibă o strategie de backup pentru acoperirea riscurilor de pierdere a informaţiilor. Şi asta nu doar din perspectiva impunerilor reprezentate de reglementările existente sau de cerinţele de auditare, ci şi din cea a riscurilor la care pot fi expuse datele din orice instituţie. Pentru a putea schiţa o astfel de strategie, respectiva instituţie trebuie să identifice o serie de activitati interne, prin care să se stabilească la ce sisteme trebuie făcut backup, cât timp ar fi necesar pentru ca să se finalizeze backup-ul, în cât timp trebuie făcută restaurarea şi dacă există nevoia unui al doilea site de salvare a datelor. Sunt cerinţe minime, dar care facilitează identificarea soluţiei care acoperă cerinţele reale şi, inerent, influenţează bugetul alocat atat pentru solutii software de efectuare a copiilor de siguranta cat si pentru solutiile hardware.

O soluţie de backup are în principal două componente: partea hardware şi partea software. Partea hardware este mediul pe care se face backup-ul. Partea software este aplicaţia care realizează backup-ul. În zona de hardware există echipamente dedicate pentru backup. Unele pot oferi redundanţă la nivel de componente şi pot avea viteze diferite de transfer al datelor. În momentul actual tendinţa pieţei este de scădere a preţului pe unitatea de stocare .

În ceea ce priveşte partea software, Microsoft are propria soluţie de backup pentru fiecare produs caruia i se adresează. Exista si alti producatori de software care au dezvoltat propriile solutii, precum McAfee, Symantec sau Acronis. Calculatoarele ce ruleaza Linux au şi ele o gama variată de soluţii de backup. De asemenea, pentru maşinile virtuale Vmware există aplicaţii de realizare a salvarilor.

O alternativă la achiziţionarea de hardware şi software pentru salvarea datelor o reprezintă contractarea unui serviciu de întreţinere a bazei de date de la o companie specializată, plătind doar un abonament lunar pentru un anumit spatiu de stocare. Avantajul este că, echipamentele aparţin provider-ului de servicii, oferind astfel o siguranţă mult mai mare şi costuri de administrare mai mici (plata lunară, fără o investiţie majoră).

Câteva soluţii software mai importante ar fi:

MS Data Protection Manager (DPM) Aceasta solutie Microsoft ofera protectie unificata a datelor pentru servere Windows, cum ar fi SQL Server, Exchange, SharePoint, virtualizare si servere de fisiere, precum si Windows pentru desktop-uri si laptop-uri.
Laptop-urile care nu stau la birou beneficiază de politici de management centralizat pentru protecţia datelor chiar dacă utilizează reţeaua internă a companiei sau se află în mişcare în afara ei. Caracteristica de recuperare a datelor în caz de incidente este foarte puternică, deoarece DPM (data protection management) oferă replicare site-to-site la un alt server DPM sau un furnizor de servicii off-site.

Symantec Backup Exec Deoarece foloseste de-duplicarea inteligentă şi o tehnologie de arhivare, aceasta aplicaţie permite protejarea mai multor date şi reducerea costurilor de stocare şi de management.

IBM Tivoli Storage Manager FastBack permite să efectum rapid recuperarea datelor pentru orice server Microsoft Windows, în orice moment şi în orice loc din organizaţie.

Sistemul integrat Oracle cu pierderi zero în recuperarea datelor: algoritmii de backup integraţi în Oracle Database trimit către sistem doar datele modificate, minimizând impactul asupra bazei de date, a traficului I/O și a încărcării de rețea. Toate prelucrările costisitoare de backup scumpe sunt transferate către dispozitiv.

Toate solutiile enumerate mai sus au rolul de a ne ajuta să economisim timp şi bani, şi să reducem riscurile de a pierde toate datele importante pentru noi sau institutie. Beneficiile aduse de oricare dintre solutii de backup sunt:
- întreruperile de activitate sa fie reduse sau chiar eliminate, în timp ce informaţiile privind sistemele virtuale sau fizice sunt securizate şi restaurate în timp cat mai scurt. Aceasta tehnologie permite, de asemenea, de-duplicarea integrată şi adaptabilă, arhivarea unificată şi recuperarea granulară pentru aplicaţiile utilizatorilor atât de pe maşinile fizice cât şi de pe cele virtuale.
- asigură protejarea continuă a datelor şi gestionarea recuperării pentru serverele Microsoft Windows, atât în centrele de date, cât şi în birourile aflate la distanţă sau în sucursale.
- elimină pierderile de date: Integrarea unică a bazelor de date permite

transportul continuu de date către dispozitiv, oferind astfel protecție în timp real pentru cele mai recente tranzacții, astfel încât bazele de date să fie restaurate fără pierderi de date.

- reface capacitatea de operare a aplicaţiilor şi a utilizatorilor la câteva minute după o pierdere de date, întreaga recuperare a datelor fiind realizată în fundal, fără impact major asupra performanţelor maşinilor sau userilor
- elimină necesitatea obişnuitelor ferestre de salvare, prin captarea în mod continuu a modificărilor de date la nivel de bloc, cu un impact extrem de redus asupra performanţei sistemelor
- planifică transferuri automate de date folosind setări flexibile, bazate pe politici, ajutând administratorii să îndeplinească cerinţele de protejare şi păstrare a datelor pentru fiecare aplicaţie în parte
- permite recuperarea oricăror resurse de date, din orice aplicaţie Windows, inclusiv Microsoft Exchange, Microsoft SQL Server, Oracle, IBM DB2 şi SAP
- optimizează utilizarea lăţimii de bandă disponibile prin strategii cum ar fi folosirea mai multor fire de execuţie, gruparea fişierelor mici şi comprimarea conform standardelor industriale
- realizează integrarea cu aplicaţiile existente de salvare pe bandă, cum ar fi IBM Tivoli Storage Manager, şi asigură un nivel intermediar de salvare pe disc, accelerând semnificativ operaţiile de salvare şi recuperare
- permite revenirea la orice moment dat adica datele privind modificarea bazei de date stocate pe sistem pot fi folosite pentru a crea copii virtuale complete ale bazei de date la orice la orice punct temporal dorit.

Ca o concluzie a celor expuse mai sus:

Riscuri

In cazul in care nu există o soluţie de protecţie a datelor sau aceasta este aleasă incorect, orice companie riscă să piarda informaţii critice pentru desfăşurarea activităţii ei, informaţii ce e posibil să nu mai potă fi recuperate. Implicit, compania poate pierde oportunităţi, clienţi, bani şi timp investit în recuperarea datelor.

În cazul unei pierderi majore, compania ar putea fi nevoită să îşi întrerupă activitatea, lucru care ar afecta productivitatea angajaţilor.

Existenţa unui backup în instituţie oferă siguranţa că putem recupera o mare parte din informaţiile pierdute sau corupte şi că activitatea nu va fi afectată de o eventuală avarie a dispozitivelor hardware sau eventuale probleme software.

Solutii

În momentul alegerii unei solutii optime de backup trebuie să luam în considerare caţiva factori importanţi pentru nevoile instituţiei, cum ar fi:

Cat de des se realizeaza backup-ul?

În funcţie de dinamica modificării şi de necesitatea (importanţa) informaţiilor, fiecare companie poate avea nevoie de actualizări mai rare sau mai dese ale backup-ului. Se poate calcula care este timpul maxim pentru care o companie poate pierde informatii, fară a afecta continuitatea serviciilor oferite. Cu cât facem mai des activitatea de salvare a datelor creşte timpul de ocupare a maşinilor, capacitatea de date stocate şi în final costurile.

Ce tip de backup trebuie utilizat?

În functie de spaţiul de stocare şi de viteza cu care informaţiile pot fi recuperare ulterior, procesul de backup poate fi facut in mai multe moduri.
Integral – se face o copie completa a datelor;
Incremental – se realizeaza initial o copie completa dupa care se salveaza doar modificarile de la ultimul backup;
Diferential – se salveaza doar modificările de la ultimul backup, integral.

Mediul pe care se stocheaza backup-ul

Acesta trebuie sa fie diferit de cel de pe care sunt copiate datele. De asemenea, este important ca acesta sa fie un mediu sigur, fiabil, redundant. Datele pot fi stocate pe benzi magnetice, hard disk-uri, storage optic sau în cloud.

Cand se realizeaza backup-ul

Momentul în care se realizează şi actualizează informaţiile trebuie să fie ales astfel încât să nu afecteze performanţa sistemelor. De obicei, acesta se realizeaza noaptea sau la sfârşitul săptămânii, deoarece procesul creşte traficul în reîea şi consumă din resursele sistemelor.

Ce este solutia Backup?

Backup-ul reprezintă un proces de copiere constant al datelor pe alte medii de stocare, altele decât cele de lucru pentru a putea fi restaurate în cazul în care cele originale se pierd sau sunt distruse. Compania de hosting sau cea care produce şi manipulează informaţiile efectuează backup-uri periodice, dintr-o data anterioară la care datele au fost valide.
Există numeroare intruziuni prin care se pierd date, pornind de la un virus ce poate corupe informaţiile sau chiar defecta hardware-ul, cât şi prin stergerea sau manipularea eronata a acestora.
In consecinta, **Backup-ul** şi refacerea acestuia reprezintă o reală necesitate a întregii securităţi a unui sistem. Prin această metodă, se pot recupera destul de uşor şi rapid datele pierdute.

De ce este important backup-ul?

Pentru că doar aşa ne putem asigura că orice probleme întâmpinăm pe parcursul activităţii noastre în mediul online, putem restaura totul! Internetul este plin de ameninţări, iar viruşii şi atacurile hackerilor nu sunt singurele motive pentru care ar trebui să avem mereu un backup. Uneori şi noi putem face o setare greşită pe interfaţa de management a maşinilor, sau şterge un fişier, caz în care rezolvam problema apărută restaurând backup-ul.

Care sunt solutiile cele mai potrivite? Backup manual sau backup automat?

Există o diferenţă între aceste două tipuri de backup. Cel automat este realizat de un soft, iar cel manual presupune copierea fişierelor şi bazelor de date într-o locatie sigură, manual şi individual.
Se recomandă folosirea backup automat pentru a nu uita că trebuie făcut luându-ne cu activităţile zinice. Un alt mare avantaj al salvărilor automate îl reprezită faptul că pot fi programate a fi făcute noaptea când serverele sunt libere de activităţile curente iar traficul în reţeaua internă este nul. Cel manual se recomanda în general pentru PC/laptopul individual.

Nu este vorba de o problemă nouă, însă creşterea explozivă a volumelor de date este principala cauză care transformă backup-ul într-o provocare specială, care trebuie abordată cu atenţia cuvenită. (IDC, de exemplu, preconizează că, în 2020, volumul de date va ajunge la o valoare totală de 35.000 de Exabytes, ceea ce înseamnă de aproximativ 29 de ori mai mult decât volumul de 1.200 de Exabytes cât a fost estimat că au fost în anul

2010.)

Creşterea rapidă a volumelor de date în cadrul companiilor se datorează, pe de o parte, multiplicării surselor de date structurate, ca urmare a înmulţirii proceselor economice informatizate, dar şi includerii şi utilizării în procesele curente a din ce în ce mai multe date nestructurate, al căror volum creşte exponenţial o dată cu explozia Web 2.0 şi a social media. În cazul instituţiei noastre cantitatea de date va creste exponenţial dacă nu, chiar exploziv o dată cu digitizarea colecţiilor (cărţi rare, manuscrise, stampe, numismatică).

Cantităţile uriaşe de date care ar trebui, teoretic, salvate/conservate fac prohibitiv costul protejării datelor. Chiar dacă preţul backup-ului pe disc a scăzut şi scade constant, acesta este încă sensibil mai mare decât cel al stocării pe bandă. Deşi avantajele tehnologiilor de backup Disk-to-Disk sunt incontestabile, multe companii continuă să îşi salveze datele pe librării de benzi. Un demers mai mult decât justificat, şi nu doar din perspectiva costurilor ci şi a fiabilităţii. Dezavantajul major al benzilor este viteza scazută la scriere sau citire şi mai ales necesitatea derulării sale până la informaţia necesară.

Avantajele incontestabile ale deduplicării

Vânzătorii de soluţii de tipul Backup-to-Disk încearcă şi reuşesc să surmonteze o bună parte din problema reprezentată de creşterile uriaşe ale volumelor de date, prin dezvoltarea de tehnologii de deduplicare din ce în ce mai eficiente. Principalele beneficii pe care deduplicarea, asociată soluţiilor de backup, le oferă sunt:

- Reducerea volumului de stocare
- Economii de lăţime de bandă
- Posibilitate de replicare a datelor automat
- Creşterea vitezei de replicare a datelor
- Restaurarea mult mai rapidă a datelor
- Scăderea consumului de energie
- Posibilitatea realizării backup-ului unor sisteme care nu puteau fi replicate anterior prin metodele clasice de backup pe bandă.

Este nevoie de mai mult

Şi totuşi, deduplicarea nu rezolvă integral toate problemele aferente

operaţiunilor de backup. Chiar dacă se foloseşte alături de tehnologii de tipul Backup Incremental sau Block-Based Backup, deduplicarea nu poate reprezenta soluţia unică pentru toate problemele care apar o dată cu migrarea accelerată a companiilor către mediile virtuale şi utilizarea din ce în ce mai intensivă a unor volume mari de date nestructurate, de tipul Social Media Analytics. De exemplu, creşterea rapidă a numărului de maşini virtuale poate pune probleme reale atunci când se trece la realizarea operaţiunilor de backup, pentru că au un impact direct atât asupra serverului (consumului de resurse CPU şi memorie) şi suporturilor de stocare (disc sau benzi), cât şi asupra lăţimii de bandă, fiind afectate viteza, respectiv durata de timp. Iar în condiţiile în care marea majoritate a companiilor au nevoie de recuperarea cvasi-instantanee, în cazul informaţiilor şi aplicaţiilor critice, problema începe să capete valenţe complexe. Mai ales atunci când în discuţie apar parametri precum Recovery Time Objectives (RTOs) şi Recovery Point Objectives (RPOs), vitali atunci când este vorba de restaurarea maşinilor virtuale.

Disaster Recovery şi Business Continuity sunt privite, îndeobşte, ca două concepte rezervate doar marilor companii, cu un volum foarte mare de clienţi si de date procesate. Cu toate acestea, blocarea accesului la date sau imposibilitatea executării anumitor operaţiuni critice pentru desfăşurarea activităţii sunt probleme care afectează drastic orice tip de companie, indiferent de dimensiunile acesteia. Iar backup-ul şi restaurarea reprezintă o etapă esenţială în stabilirea unui plan eficient şi realist de recuperare a datelor în caz de dezastru.

Aceasta a fost partea teoretică. Acum voi trece la analiza unui caz al unei Instituţii de educaţie unde lucrează Domnul Rezolvă Tot şi a soluţiei impusă de Doamna contabila Nu am bani:

In trecut: se facea back-up doar la baza de date Aleph pe o unitate de banda care s-a defectat datorită vechimii şi a folosirii zilnice.

Cum costul unei unităţi de banda este foarte ridicat, domnul Rezolva tot a început să analizeze mai multe soluţii de back-up care se puteau preta la activitatea şi necesităţile instituţiei în cauză şi extinderea salvarilor şi la celelalte servere necesare funcţionării activitaţii Instituţiei.

Back-up la ei se face în mai mulţi paşi, după cum urmează:
1. Script de Aleph prin care se face export local la baza sa de date;
2. Serverul Aleph vechi (a ramas doar cu numele pentru că a fost reinstalat şi actualizat sistemul de operare Linux de pe el şi a fost sters programul de Aleph pentru a elibera spaţiu), pe la ora 2 noaptea aduce modificările din exportul facut pe serverul principal, pe el;
3. Se scrie pe casetă ca atare, apoi se verifică caseta;

Cum unitatea de casetă dadea mereu erori la scriere, a cerut şi s-a achizitionat un HDD extern şi astfel are o copie a bazei de date pe acest HDD şi în acelaşi timp şi spaţiu de manevră deoarece spaţiul pe server era limitat şi nu se puteau achizitiona 6 HDD mai mari care sa lucreze în RAID aşa cum trebuie şi cere serverul.

Fac precizarea că, soluţia aleasă de a cumpara un HDD extern a fost adaptată conditiilor financiare din unitatea culturală în cauză, costul unui HDD extern (cca. 300 lei) fiind de cca. 10-15 ori mai mic decat ar fi costat o unitate de casetă şi casetele aferente (între 2.800-6.000 lei) sau costul a 6 HDD SCSI a 753 lei bucata câte ar trebui cumpărate pentru a înlocui pe cele de 36GB din dotare dar, dezavantajul solutiei aleasă este însă fiabilitatea mult mai redusă.

Acum: continuam procesul
4. Se face o singura arhiva mare criptată pe hdd extern
5. Daca pasul 4 s-a terminat cu succes, se copiaza arhiva criptată pe un server extern aflat într-o alta instituţie şi locaţie.
6. Se trimite mail cu logul operaţiunilor. In logul respectiv a fost programat să scrie ora începerii fiecărui pas şi când s-a terminat şi astfel el poate urmări modul în care decurge salvarea.

Serverul Instituţiei pe care a fost Aleph-ul fiind mai vechi, procesul de criptare decurge foarte lent, datorită faptului că procesorul şi memoriile sunt de generaţie foarte veche (instructiuni pe secunda IPS si magistrala de date FSB fiind mult mai mici decât la actualele procesoare aflate în telefoanele inteligente de top).

În felul acesta se face back-up în mai multe moduri, neimplicâd costuri suplimentare dar, consuma mult, mult timp.

Nu a protejat doar baza de date din Aleph ca pană de curând ci a analizat şi restul serverelor şi a organizat activităţile de salvari dupa cum urmează:
Serverul Aleph - sistemul integrat de biblioteca care reprezintă "bussinesul" unei biblioteci are salvarea integrală inclusiv setarile sistemului de operare

pe serverul vechi (bătrânul Aleph) şi în cloud pe un server FTP pus la dispozitie de către Norişorul SA (server care nu se afla în locaţia unde-şi desfăşoară activitatea principală şi este deci şi pe post de Disaster Recovery).
Serverele Domain Controler, pe scurt DC1 si DC2, cele care se ocupă de securitatea din domeniul pus la punct de Domnul Rezolvă Tot îşi fac salvările încrucişat, fiecare pe serverul opus;
Serverul de Contabilitate, serverul Kaspersky (antivirus), serverul pe care este siteul instituţiei, serverul de email şi serverele de camere au acum o salvare pe o unitate de stocare externa situata însă tot în incinta camerei serverelor.

In viitor: speră să obţină spaţiu de stocare mai generos pe serverele Norisorul SA ca să poată muta şi salvările siteul Instituţiei şi a celorlalte servere de pe unitatea de stocare externă în cloudul extern, deci şi în altă locaţie fizică.

Aceasta a necesitat din partea lui o activitate susţinută de studiu individual, de cercetare şi analiză a soluţiilor de stocare şi de salvare a datelor, de analize din punct de vedere financiar a diverselor solutii software şi hardware posibile de adoptat din cele prezentate mai sus (aceasta a fost partea cea mai usoara intrucat fondurile alocate de doamna Nu am Bani au fost apropiate de 0 şi deci analiza a trecut rapid peste această etapă) şi au fost luate în calcul doar soluţiile software gratis puse la dispoziţie de către Microsoft, Oracle şi Linux. Următorul pas a fost cel de analiză a resurselor hardware care puteau fi orientate în alte activităţi necesare procesului de salvare (de exemplu, vechiul server Aleph care a fost refolosit ca unitate de stocare şi unitatea de stocare extenă pe care s-au facut salvari de la scanări vechi care s-au predat beneficiarului şi care după mutarea imaginilor scanate şi stocate pe ea rămasese nefolosită) de cooperare interinstituţionala atât cu firma care asigură întreţinerea serverelor, Biţii SRL cât şi Norişorul SA, care asigură atât linia protejată şi securizată a datelor de la sediul instituţiei la sediul Norisorul SA cât şi spatiul de stocare în cloudul din data centreul acesteia.

Au fost peste 200 de emailuri schimbate între el şi diverse persoane din instituţiile colaboratoare deoarece au fost probleme în a obţine gratuit spaţiul de stocare, a liniei de comunicaţii între cele două instituţii care a avut şi mai are încă probleme cu echipamente depăşite tehnologic şi a multor altor probleme care au apărut şi au trebuit să fie manageriate şi solutionate pentru a obţine soluţii valide.

Situaţia salvărilor a fost testată pe 26 iunie când s-a defectat serverul DC1 (defect pe placa de bază conform testelor efectuate de domnul Rezolvă Tot şi de firma Biţi SRL). Pentru că el conştientiza rolul şi importanţa DC1 în structura reţelei (în caz de nefuncţionare a sa, userii nu se mai puteau autentifica în Domeniu, calculatoarele nu-şi mai puteau lua adrese IP date de serviciul DHCP şi în felul acesta nu mai puteau intra in Reţea şi nu mai aveau acces la Internet, la emailuri, etc.), rolul său era monitorizat şi dublat iar în momentul defectarii a fost preluat de către DC2 şi s-au restaurat datele din salvările aflate pe DC2. În momentul de faţă reţeaua e funcţională, nu au fost întreruperi în funcţionarea sa, dar lucrează în regim de **AVARIE**. Cum nu se poate lucra sigur doar cu un singur domain controller, respectiv DC2, care de fapt nici nu e server cu adevarat (pentru ca nu i s-au dat bani de achizitii nici în alte vremuri) ci un calculator normal cu rol de server, care din punct de vedere al fiabilitatii nu e la fel ca un server. Pentru a fi acoperiţi au împrumutat de la firma care ne face serviceul un server pe post de DC1 şi funcţionează cu un server de împrumut. De aceea s-a afirmat că reţeaua lucrează în regim de AVARIE.

Concluzie: domnul Rezolvă Tot are salvări facute la principalele servere şi la baza de date de date care conţine informaţii utile Instituţiei. Soluţia de back-up e viabilă şi chiar a fost testata cu succes într-un caz real, de avarie gravă, asa cum am precizat mai sus cand şi-a încetat activitatea serverul nostru DC1.

Fără investiţii serioase în infrastructura veche de mulţi ani aflată în Instituţie vor fi din ce în ce mai dese incidentele şi la un moment dat structura va cădea DEFINITIV.

In încheiere işi permite sa mai analizeze cateva vulnerabilitati ale infrastructurii de Tehnologia Informatiei si Comunicatii a Instituţiei.

- sunt necesare servere noi, licente noi pentru că şi licentele de Windows Server 2003 pe care le foloseşte au expirat din punct de vedere al updatelor de securitate (14 iunie ac când Microsoft l-a scos din serviciul de asistenţă şi update), swichuri noi cu management pentru a putea securiza şi izola noile subretele apărute (au fost montate routere WIFI la sălile de lucru cu publicul, ba chiar şi unele birouri au cerut propia reţea WIFI), surse UPS pentru a susţine activitatea serverelor şi a swichurilor în cazul penelor de curent care au devenit o mare problemă din cuza căderilor repetate a tensiunii electrice în reţeaua Enel care a fost extinsă dar nu a fost modernizată.

- o alta vulnerabilitate majora a retelei Instituţiei o reprezinta faptul că instalaţia de climatizare a incintei unde funcţionează serverele nu este dublata, singura instalaţie care lucrează fiind una Fujitsu veche şi ea de 5 ani. Și acesta este suprasolicitată, lucrează non-stop, fie iarnă fie vară pentru a asigura 18-20 C în incinta locaţiei serverelor.

- pentru că şi reţeaua de comunicaţii a Instituţiei este tot la fel de ancestrală şi tot oarecum în custodia sa aminteşte că este impetuos nevoie de o centrală nouă deoarece modelul Centrala telefonică este scos de mult timp din fabricaţie şi nu se mai fac piese de schimb pentru el, în cazul unei defecţiuni putând să apară întreruperi in comunicare. Ce a depins de el şi de firma care asigură întreţinerea a făcut, revizii şi curaţări periodice, i-a prelungit viaţa cât se va putea de mult printr-o îngrijire ca la carte, dar timpul lucrează şi toate lucrurile îmbătranesc, nu numai oamenii.

WEBliografie:

Diverse siteuri unde am găsit şi structurat multe informaţii dupa cum urmeaza:

http://www.microsoft.com
http://www.oracle.com
https://academy.oracle.com/
http://www.hp.com
http://www.dell.com
https://ibm.com/
http://ittrends.ro
http://www.marketwatch.ro

7 iulie 2015
Ovidiu Alexandrescu