ACADEMIA OAMENILOR DE ȘTIINȚĂ DIN ROMÂNIA

BIBLIOTECA DIGITALĂ PENTRU ROMÂNII DE PRETUTINDENI

SECURITATEA INFORMAȚIEI DIGITALE ÎN CLOUD

COORDONATOR:
PROF. UNIV. DR. DOINA BANCIU

CSII dr. ing. Adrian-Victor VEVERA

2018

SECURITATEA INFORMAȚIEI DIGITALE ÎN CLOUD

CSII dr. ing. Adrian-Victor VEVERA

Securitatea informației digitale în Cloud

În general, piața de cloud computing din România este dominată de furnizorii internaționali, însă segmentul de stocare în cloud rămâne, de departe, cel mai promițător pentru providerii locali, fie că vorbim despre companii de telecom, fie că vorbim despre centre de date.

Printre bunele practici care să asigure protecția informației digitale în contextul stocării acestuia pe sistem de mari dimensiuni de tip cloud putem enumera:

Accesul – Furnizorii de servicii cloud trebuie să poată demonstra că pot asigura controlul și supravegherea accesului personalului, mai ales în cazul procesării datelor importante și confidențiale.

Conformitate – Deși clienții vor fi întotdeauna responsabili pentru propria conformitate cu regulile, felul în care este împărțită responsabilitatea între client și furnizor trebuie să fie clar definită.

Certificarea aplicației – Certificatele de securitate sunt esențiale în procesarea informațiilor în cloud pentru a certifica faptul că aplicația pentru certificatul SSL este autentică.

Proveniența datelor – termenii contractuali trebuie să fie clari în privința conformității cu regulile și legile locale. Acest aspect este esențial în Europa, acolo unde există reglementări care militează împotriva uniformității.

Segregarea – Serviciile de cloud operează într-un mediu care împarte capacitatea de calcul, managementul datelor, comunicarea și facilități de securitate, de aceea este esențial ca furnizorul să ofere proceduri de continuă monitorizare și procesare a datelor.

Data recovery – Contractele de cloud trebuie să stipuleze că furnizorul trebuie să asigure o recuperare completă a operațiunilor în cazul unui incident și să asigure prin SLA un număr maxim de minute de downtime în funcție de tipul incidentului.

Transferul aplicațiilor – dacă transferul în cloud se realizează relativ simplu și reprezintă o sursă semnificativă de diminuare a costurilor, transferul în sens invers sau între diferite tipuri de cloud sau furnizori este mult mai dificil; de aceea, condiții contractuale care să asigure interoperabilitatea softului la transferul între diverse medii de operare sunt esențiale.

Business continuity – una dintre cele mai frecvente tendințe este consolidarea centrelor de date, de aceea, contractele pentru servicii de cloud trebuie să includă aspecte care să stipuleze faptul că transferul de date între diverse centre trebuie să fie asigurat oricând apar schimbări majore în felul în care operează business-ul.

Într-un model de securitate a responsabilității partajate, furnizorul de cloud computing și consumatorii de cloud computing au fiecare un rol important în asigurarea securității infrastructurii și aplicațiilor livrate în cloud computing.

Cu toate acestea, indiferent de modelul folosit: Infrastructură ca serviciu (IaaS), Platformă ca serviciu (PaaS) și Software ca serviciu (SaaS) - clientul este, în general, responsabil pentru securitatea datelor și accesul/identitatea utilizatorilor (Figura 1).

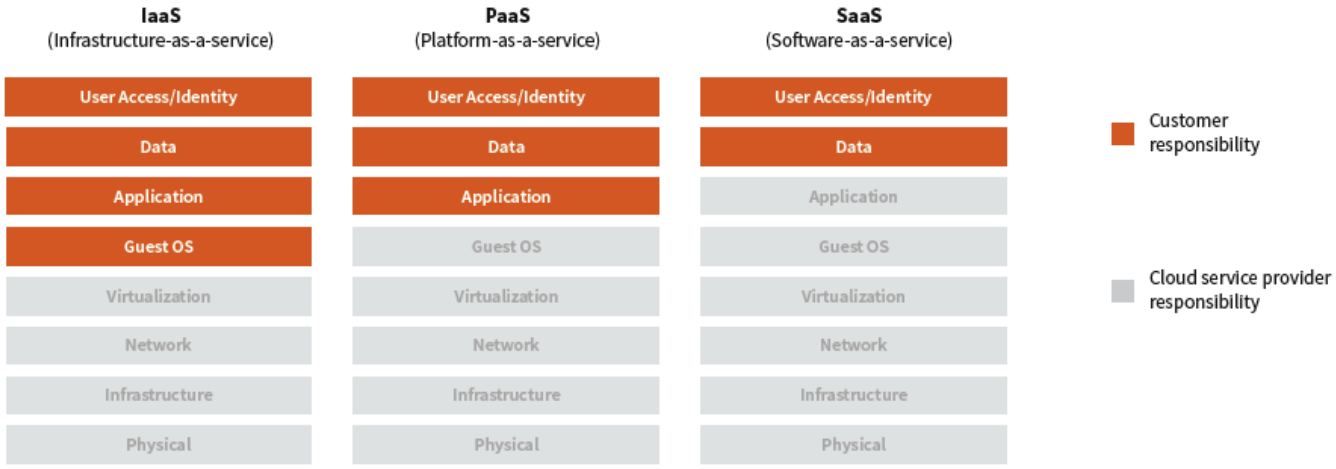

Figura 1. Modul de răspundere partajată pentru securitatea în Cloud Computing

(Sursa: Oracle and KPMG - Cloud Threat Report, 2018)

Dacă în perioada incipientă a cloud-ului acesta era perceput ca fiind similar cu zona DMZ (Demilitarized Zone - este o arhitectură conceptuală de rețea în care serverele cu acces public sunt plasate separat pe un segment izolat de rețea), cu timpul cloud-ul a devenit din ce în ce mai utilizat și în zona de "intranet" extinzându-și utilitatea în cadrul organizațiilor. În general multe dintre amenințările la adresa cloud computing sunt aceleași cu cele cu care ne-am confruntat până la apariția cloud-ului, însă s-ar putea ca acestea să se manifeste în moduri noi sau să prezinte un risc mai mare. Nu există echipamente dedicate pentru a securiza cloud-ul, clienții trebuie să perceapă serviciile cloud și securitatea în cloud ca o problemă de securitate în ansamblul ei, pe întreg lanțul de furnizare de servicii. În Tabelul 1 sunt descrise tipuri de amenințări în cloud și modul de rezolvare ale acestor amenințări.

Tabelul 1. Tipuri de amenințări și contramăsuri

Tip de amenințare	**Contramăsuri**
Malware	• appliance-uri hardware sau software împreună cu agenții instalați la nivel de end-device-uri, • training specific efectuat de către utilizatori cu privire la folosirea internetului, mail-ului etc.
Amenințări interne	• verificarea cu atenție a backgroundului fiecărui potențial angajat, • pentru angajații existenți se recomandă rotația pe posturi, • monitorizare și supraveghere continuă.
Atacuri externe	• contramăsurile includ securizarea echipamentelor, hypervizoarelor și a mașinilor virtuale la nivel de firmware / sistem de operare, • actualizarea continuă a politicilor de securitate.
Atacuri te tipul Man-in-the-Middle	• criptarea datelor în tranzit (mișcare) incluzând și activități de autentificare.
Social Engineering	• training.
Furtul sau pierdere de dispozitive	• criptarea datelor stocate pe aceste dispozitive, o inventariere și monitorizare a tuturor echipamentelor, posibilitatea de a șterge (wipe) datele de la distanță.
Dezastre naturale	• providerii de cloud trebuie să asigure multiple măsuri de redundanță pentru toate sistemele si componentele din

Tip de amenințare	Contramăsuri
	Datacenter, incluzând ISP si utilități. De asemenea trebuie să existe strategii privind "Disaster Recovery (DR) și Business Continuity Management (BCM)".
Lipsa accesului la audit	• în cazul în care providerul refuză să permită clientului dreptul de a audita facilitatea, clientul trebuie să se poată baza pe auditul făcut de către o terță persoana de încredere.
Escaladarea privilegiului	• implementarea de tehnici de autentificare și control al accesului; • implementarea de soluții de tipuri SIEM (Security Information and Event Management), SIM (Security Information Management) sau SEM (Security Event Management).
Contractual Failure	• Pentru o protecție suplimentară, clientul trebuie să ia în considerare backup-urile offsite cu scopul de a refacere sistemul informatic în alt cloud.

Recuperarea datelor în caz de dezastru în cloud (Cloud DR - Disaster Recovery) reprezintă cea mai importantă problemă și este o strategie de backup și restaurare care implică stocarea și păstrarea copiilor de siguranță ca măsură de securitate. Scopul Disaster Recovery este acela de a oferi unei organizații o modalitate de a recupera datele în cazul pierderii acestora în urma unei catastrofe naturale sau provocate de om. În Figura 2 este prezentată replicarea la nivel de storage a datelor și protecția/securizarea informației pe mai multe nivele și anume:

1 – echipamente dedicate de securitate (firewall, IDS/IPS, DDOS, Web Security appliance, Web application Firewall etc.);

2 – protocoale folosite în cloud pentru izolarea rețelelor clienților (NVGRE (Network Virtualization using Generic Routing Encapsulation);

3 – actualizarea sistemelor de operare pe servere, mașini virtuale;

4 – replicare date pentru a asigura înalta disponibilitate (high availability).

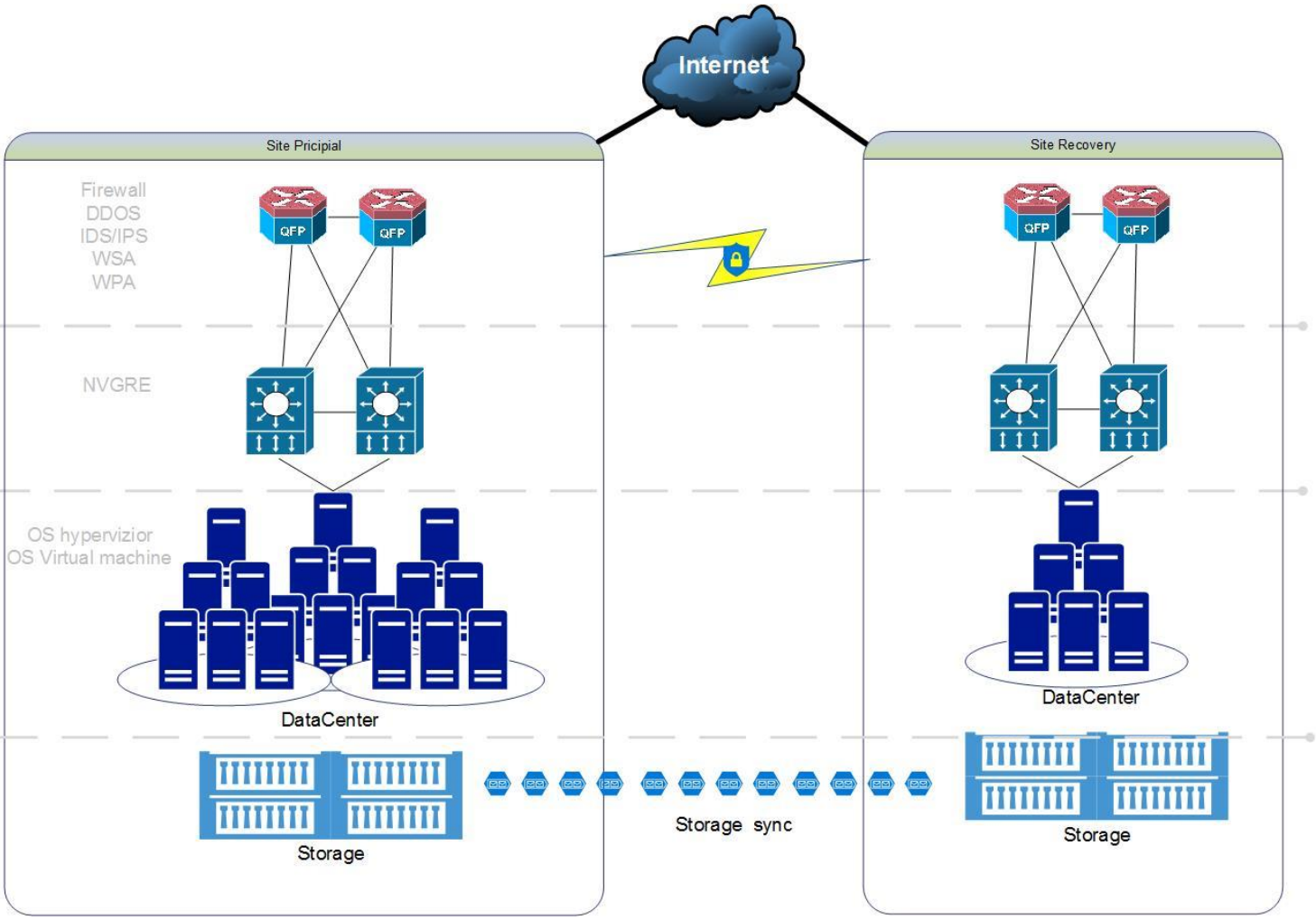

Figura 2. Replicarea la nivel de storage a datelor