



**Cofinanțat de
Uniunea Europeană**



Proiectul Wallachia eHUB (WEH)

ID proiect: EC/101083410 – WeH; POCIDIF/1147/2/1/161799

Str. Italiană nr. 28, sect. 2, București - România

weh@spiruharet.ro weh.spiruharet.ro

Codul proiectului: EC/101083410– WeH/ și POCIDIF/1147/2/1/161799

Titlul proiectului: Wallachia eHUB (WEH)

WP 3. Servicii de dezvoltare a competențelor și de formare profesională (Skills Development and Training Services)

Material de curs pentru sesiunea de instruire Servicii Cloud (Microsoft Azure, Google Workspace)

Întocmit,

Manea Mihai-Laurențiu

USH_Trainer de coordonare a transformării digitale

Februarie 2025



Introducere:

Soluțiile tehnologice cunoscute sub denumirea de cloud computing, reprezintă o schimbare fundamentală în felul în care sunt dezvoltate, livrate, actualizate, întreținute și plătite serviciile IT din cadrul organizațiilor moderne. Cloud computing semnifică convergența a două tendințe majore ale IT-ului zilelor noastre: eficiența IT - unde puterea calculatoarelor moderne este utilizată mai eficient printr-o scalare înaltă a resurselor de hardware și software și agilitatea de business – unde tehnologia informațională poate fi folosită ca instrument competitiv pe piață prin livrare rapidă, loturi paralele de procesare, utilizarea instrumentelor de inteligență a afacerilor, care necesită calcul intensiv și aplicații mobile interactive și care răspund în timp real cerințelor utilizatorului.

Cuvântul provine din limba engleza, unde înseamnă “nor” și sugerează un spațiu de stocare virtual, care se afla pe un server. Adică stochezi datele într-un loc pe care nu-l vezi cu ochii tai. A utiliza cloud este ca și cum ai utiliza calculatorul altcuiva. Fără să-ți pese de achiziție, mentenanța, curent sau upgrade.

Există probabil atâtea definiții câți comentatori/autori ai subiectului. Definiția formală a ceea ce înseamnă conceptul de cloud computing este următoarea: este un model de organizare al serviciilor IT, care presupune că serviciile de prelucrare (hardware și software) sunt livrate la cerere către clienți prin intermediul rețelelor de calculatoare, într-o manieră de autoservire, independent de locația dispozitivului utilizat. Resursele necesare pentru a livra un serviciu la un nivel înalt de calitate sunt distribuite, scalabile în mod dinamic, livrate rapid prin virtualizare și lansate cu minim de



interacțiune din partea furnizorului de servicii. Utilizatorii plătesc pentru acest serviciu ca o cheltuială operațională, fără a necesita investiții semnificative de capital inițial. Serviciile de cloud utilizează un sistem de măsurare care alocă resursele de calcul în blocuri corespunzătoare nivelului de prelucrare solicitat. Cloud computing este un subiect vast, care cuprinde mai multe subiecte diferite. Pentru a descrie în mod adecvat ofertele de cloud computing, trebuie să tratăm în detaliu elemente de infrastructură, arhitecturi orientate spre servicii, rețele sociale, protocoale de comunicare, standarde, interfețe de programare aplicații (API), și zeci de alte subiecte.

Cloud computing-ul este conceptul care aduce cele mai mari schimbări în evoluția dinamică a tehnologiei informației și comunicației (IT&C). Zilnic oamenii generează, accesează, prelucrează și stochează seturi de date noi, beneficiind de mai multă putere de procesare decât oricând înainte.

Companiile care furnizează servicii de tip cloud le permit utilizatorilor să păstreze fișierele și aplicațiile pe servere la distanță și să acceseze toate datele prin internet. Astfel, datele, munca și aplicațiile unei persoane sau companii sunt disponibile pe orice dispozitiv care se conectează la internet.

Pentru corporații, o consecință profundă a acestui consum digital în creștere este necesitatea de a investi permanent sume de bani în echipamente de prelucrare și stocare. Serviciile cloud computing devin adevărate incubatoare pentru noile aplicații, menite să răspundă cererii de obținere rapidă de informații și acces facil la acestea.

Când o companie alege să „se mute în cloud”, înseamnă că infrastructura sa IT este stocată în afara sediului, într-un centru de date gestionat de furnizorul



de cloud computing. Din acel moment, furnizorul de servicii cloud are responsabilitatea de a gestiona infrastructura IT a clientului.

Caracteristicile esențiale ale tehnologiilor cloud:

În domeniul tehnologiilor informaționale, abstractizarea este o tehnică de gestionare a complexității sistemelor informatice. Scopul său este de a stabili un anumit nivel de complexitate care poate fi înțeles de un utilizator al sistemului, suprimând detaliile esențiale care guvernează nivelul de lucru la care utilizatorul are acces. Cloud computing abstractizează detaliile de implementare a sistemului față utilizatori și dezvoltatori. Aplicațiile rulează pe sisteme fizice care nu sunt specificate, datele sunt stocate în locații care nu sunt cunoscute, administrarea sistemelor este externalizată, iar omniprezența utilizatorilor la acele aplicații nu este vizibilă decât în zona de cloud închiriată de companie.

Localizarea spațiului de stocare și caracteristicile tehnice nu sunt vizibile utilizatorului, dar fiecare user are acces instantaneu la datele sale, oricând și de oriunde: de pe calculator, laptop, tableta, telefon, LCD. Datele respective pot fi documente, imagini, emailuri, chiar website-uri și platforme de comunicare.

La ora actuală, printre cele mai utilizate servicii în cloud se numără:

- serverele;
- spațiul de stocare;
- bazele de date (stocare, backup și preluare de date);
- rețelistica;
- programele software;



- crearea și testarea aplicațiilor;
- e-mail-ul;
- streamingul audio și video;
- livrarea de software la cerere;
- diverse analize și informații de afaceri.

Printre cei mai cunoscuți furnizori de servicii de cloud computing se numără:

- Google Cloud
- Amazon Web Services (AWS)
- Microsoft Azure
- IBM Cloud
- Alibaba Cloud
- Dell Cloud
- Oracle Cloud

Principalele beneficii și limitări ale cloud-ului:

Caracteristicile fundamentale prezentate anterior determină o serie de avantaje de care pot beneficia utilizatorii tehnologiilor cloud, pe care le expunem succint în această secțiune, o parte din ele fiind detaliate în capitolele următoare. Abilitatea tehnică a furnizorilor de cloud de exploatare la un nivel ridicat a echipamentelor de calcul, precum și mediul concurențial destul de agresiv, determină un nivel redus al prețurilor pentru care sunt comercializate serviciile cloud. Clienții beneficiază astfel de o prețuri mici comparativ cu costul total de apartenență al puterii de calcul similare pe care ar trebui să o implementeze local (on-premise). Datorită pachetelor predefinite de mașini virtuale și software preinstalat utilizatorii vor beneficia



de un acces mai ușor la serviciile informaționale de care au nevoie pentru desfășurarea activităților. De exemplu, pentru a instala un server de baze de date on-premise este nevoie de un server dedicat pe care trebuie instalat un sistem de operare, configurate servicii specifice de stocare, instalare de aplicații prerechizite, instalarea aplicațiilor pentru bazele de date și configurarea și securizarea corectă a acestora. Toate aceste operațiuni necesită licențe, timp și oameni specializați. În cloud se poate alege un pachet predefinit de server care să aibă preinstalat sistemul de baze de date dorit. În felul acesta beneficiarul nu va plăti licențe sau timpul necesar instalării și configurării ci doar timpul de utilizare a respectivei mașini virtuale fiindu-i în acest fel mult mai ușor să aibă acces la serviciul de baze de date dorit.

Beneficiile Cloud Computing:

1. *Eficiența Costurilor*: Reducerea cheltuielilor de capital și transformarea acestora în costuri operaționale, cu plata doar pentru ceea ce este utilizat.
2. *Flexibilitate și Mobilitate*: Accesul la date și aplicații de pe orice dispozitiv conectat la internet, oferind libertate și mobilitate.
3. *Securitate Avansată*: Furnizorii de servicii cloud investesc în măsuri de securitate pentru protejarea datelor utilizatorilor.
4. *Actualizări și Mentenanță Automată*: Furnizorii gestionează actualizările de securitate și întreținerea infrastructurii, eliberând utilizatorii de aceste sarcini.



Avantajele și dezavantajele utilizării cloud-ului

Avantajele cloud-ului:

- colaborare mai ușoară – editarea colaborativă a documentelor în mediul cloud permite colaborarea în timp real și reduce necesitatea de trimitere a versiunilor corectate ale fișierelor,
- acces din browser – o platformă, precum Google Workspace, poate fi accesată de pe orice dispozitiv: de pe un computer cu Windows, Linux, macOS sau de pe un smartphone.
- stabilitate și securitate – fișierele și datele din cloud sunt protejate prin parolă și pot fi protejate și mai bine prin mecanisme de securitate suplimentare; în cazul deteriorării sau furtului computerului companiei, datele vor fi în continuare în siguranță în cloud;
- controlul accesului – administratorul poate controla cu ușurință care persoane au acces la fișierele și proiectele companiei și poate gestiona nivelul permisiunilor,
- spațiu pe disc și putere de calcul – resursele cloud sunt aproape nelimitate; putem folosi oricât de mult spațiu și putere avem nevoie,
- servicii de accelerare a dezvoltării – în cazul platformelor cloud pentru dezvoltători, furnizorii de servicii oferă sute de servicii pe care puteți rula propriul cod sursă și puteți crea și mai repede un site web, o aplicație mobilă sau un program avansat



- Scalabilitate: Resursele pot fi ajustate rapid în funcție de cerințe, permițând companiilor să răspundă rapid la schimbările de cerere.
- Costuri Reduse: Elimină necesitatea de a investi în hardware și infrastructură, reducând costurile operaționale.
- Accesibilitate: Permite accesul la resurse de oriunde și oricând, cu condiția unei conexiuni la internet.
- Securitate: Furnizorii de servicii cloud oferă măsuri avansate de securitate pentru a proteja datele și aplicațiile.

Dezavantajele utilizării cloud-ului

Cloud-ul are, de asemenea, puncte slabe, iar cele mai frecvente argumente „împotriva” cloud computing includ:

- dependență de furnizorul de servicii – cloud-ul este un model în care cumpărăm acces la resurse care aparțin fizic furnizorului. Accesul la resursele cloud necesită o conexiune stabilă la internet. Dacă furnizorul are o defecțiune, accesul la datele noastre din cloud va fi dificil sau imposibil;
- securitate – o problemă care generează multe dezbateri. Furnizorii populari de servicii cloud (de exemplu, GCP, AWS) îndeplinesc o serie de cerințe de securitate. Există preocupări legate de securitatea și confidențialitatea datelor stocate în cloud, aceștia sunt supuși periodic unor audituri; cu toate acestea, datele din cloud se află pe dispozitivele furnizorului, unde este dificil să introducem propria securitate suplimentară;
- un model de facturare mai complicat – facturarea pentru serviciile cloud se desfășoară pe baza unui alt model decât atunci când utilizăm propriul



echipament fizic, ceea ce poate fi dificil la început; în cazul pachetelor de servicii pentru companii (de exemplu, Google Workspace – e-mail de firmă, cloud drive) există mai multe tipuri de licențe la alegere, iar plata depinde de numărul de posturi; costul serviciilor de infrastructură în cloud (de exemplu, Google Cloud) depinde de consumul în minute sau secunde;

- plata în exces pentru servicii ca urmare a unei configurații slabe – în cazul cloud-ului, este bine să alegem serviciile în funcție de nevoi și, foarte important, să le configurăm corect. În cazul persoanelor care nu au experiență în operarea serviciilor cloud, este mai bine să profite de ajutorul unui partener certificat, pentru că altfel pot fi expuși la costuri inutile și foarte ridicate;
- necesitatea de a introduce modificări în modul de lucru – implementarea unei soluții cloud ar trebui să fie asociată cu o schimbare parțială a modului de lucru, creșterea gradului de conștientizare a angajaților despre cloud și dobândirea de noi competențe (de exemplu, DevOps în cazul infrastructurii în cloud), ceea ce înseamnă cheltuieli financiare suplimentare. Companiile au un control limitat asupra infrastructurii și serviciilor furnizate de terți.

În cazul în care apar probleme majore de disponibilitate a serviciilor furnizorii de cloud sunt obligați să stipuleze în contracte un set de despăgubiri care se calculează de obicei ca procent din factura de servicii aferente perioadei de facturare agreeate fără a depăși 100% din valoarea facturii pe care ar trebui să o plătească beneficiarul serviciilor. Responsabilitatea de a informa o întrerupere revine în sarcina clientului de cloud, care trebuie să informeze furnizorul în timp cât mai scurt de la sesizare cu privire la natura indisponibilității și durata de manifestare a acesteia. Furnizorii de cloud nu sunt obligați să informeze voluntar consumatorii despre eventualele



întrerupere, în afara ferestrelor de mentenanță care trebuie să fie anunțate la intervale suficiente de timp în așa fel încât să permită clientului o dozare a activităților de procesare în afara acelor perioade. Transparența este una din cheile încrederii în livrarea serviciilor de cloud, de aceea fiecare furnizor pune la dispoziția publicului larg o pagină de internet cu starea curentă a serviciilor precum și istoricul întreruperilor, motivarea acestora și metodele de remediere:

- Google Cloud Status: <https://status.cloud.google.com/>
- Amazon - Service Health Dashboard - <http://status.aws.amazon.com/>
- Microsoft Azure Status: <http://azure.microsoft.com/en-us/status/>

Principalele limitări ale cloud computing-ului specificate de furnizorii specializați în contractele legate de furnizarea serviciilor și calitatea acestora sunt legate de ferestrele anunțate de întreținere, forța majoră, elemente de securitate și schimbări ale API-urilor. Întreținerea echipamentelor de calcul implică, indiferent de modul lor de organizare, o serie de întreruperi și disfuncționalități. Modelul ciclului de viață al unui sistem de operare implică o îmbunătățire continuă a anumitor componente (updates) care, în funcție de rolul lor, pot solicita utilizatorului repornirea sistemului de operare pentru aplicarea lor corectă. Mașinile fizice sau virtuale din cloud au la rândul lor nevoie de reporniri planificate a sistemelor de operare, timpul de neoperare al dispozitivelor respective fiind anunțat din timp de furnizor și nu este considerat din punct de vedere contractual o întrerupere excepțională de furnizare a unui serviciu. Dacă apar probleme, care necesită un timp



suplimentar de rezolvare față de cel planificat, atunci intră în acțiune clauzele de indisponibilitate.

Securitate și riscuri în cloud

Cloud-ul generează multe întrebări de natură juridică, mai ales când vine vorba despre prelucrarea datelor cu caracter personal. Prevederile art. 4 din Legea GDPR indică faptul că prin prelucrarea datelor se înțelege orice operațiune efectuată asupra acestor date: colectare, înregistrare, organizare, structurare, stocare, modificare, vizualizare, difuzare, inclusiv în cadrul sistemului IT. Lista este deschisă – deci se presupune că oriunde există informații despre angajați, clienți, contractanți sau utilizatori ai aplicației, are loc prelucrarea datelor cu caracter personal.

Trebuie subliniat faptul că, în cazul procesării datelor în cloud, operatorul datelor cu caracter personal este în continuare compania și nu furnizorul de servicii cloud. Operatorul este responsabil pentru încredințarea datelor entității corespunzătoare care îndeplinește reglementările în vigoare.

Iată ce trebuie să luăm în considerare atunci când alegem un furnizor de servicii cloud:

- localizarea fizică a centrelor de date – orice companie care operează într-o țară UE și, prin urmare, supusă GDPR, trebuie să aleagă un furnizor de servicii care oferă un centru de date în Spațiul Economic European (SEE);
- condițiile de furnizare a serviciilor de către furnizor – trebuie să luăm cunoștință de condițiile de prelucrare și securitate a datelor furnizate de furnizorul de servicii; se întâmplă ca unii furnizori de servicii cloud să coopereze cu organizații terțe, ceea ce implică riscul prelucrării datelor în



afara SEE de către organizații necunoscute de operatorul de date. Riscuri legate de performanță și funcționalități. Clienții de cloud trebuie să se asigure în momentul în care aleg un serviciu cloud că au testat suficient de bine performanțele serviciului și că funcționalitățile sunt corespunzătoare specificului proceselor de afaceri ale companiei. Majoritatea furnizorilor de cloud pun la dispoziția clienților versiuni de evaluare a unor funcționalități de cloud, pentru efectuarea implementărilor pilot și definirea planurilor și strategiilor de implementare, migrare și crearea documentațiilor suport. De asemenea este foarte importantă cunoașterea tuturor funcționalităților oferite de anumite servicii. De multe ori, firmele aleg anumite planuri de servicii care oferă funcționalități limitate dar la un preț mai redus, făcând dificilă ulterior dezvoltarea unor funcționalități personalizate. Alteori, clienții au cunoștințe detaliate despre anumite aplicații și servicii implementate local, aleg o soluție similară din cloud și după o perioadă de timp constată că le lipsesc anumite componente cheie de dezvoltare, personalizare și administrare a serviciilor. Serviciile și aplicațiile cloud nu au întotdeauna implementate toate funcționalitățile, sau anumite funcționalități nu pot fi personalizate sau administrate asemănător cu cele din implementările locale, dând naștere nemulțumirilor unor categorii de utilizatori.

- standarde tehnice și standarde de securitate – furnizorii de servicii cloud sunt supuși prevederilor de securitate și auditurilor efectuate de entități independente; pentru a furniza în mod legal servicii, un furnizor de servicii trebuie să îndeplinească două standarde de bază: ISO/IEC 27001 privind gestionarea securității informațiilor și ISO/IEC 27018 privind securitatea datelor cu caracter personal în cloud,



- un contract scris cu furnizorul de servicii – operatorul de date trebuie să încheie un contract scris cu furnizorul de servicii cloud privind încredințarea prelucrării datelor cu caracter personal; operatorul trebuie să se asigure că contractul conține informații despre ce entități și în ce măsură vor avea acces la datele stocate în cloud și dacă aceste entități îndeplinesc cerințele de securitate necesare.

În seria sa de mituri despre cloud, Smith (2014) specifică faptul că în cazul în care neîncrederea în disponibilitatea serviciilor cloud și a confidențialității datelor, în contextul complexității și 76 lisei de transparență, se poate alege calea implementărilor de cloud hibrid. Latura ironică a acestei idei are la bază dualitatea dintre complexitate și control. Arhitecturile de rețea foarte complexe sunt mai greu de controlat, atât de cei care le implementează, cât și de cei care încearcă să le înțeleagă pentru a le exploata vulnerabilitățile. Lipsa transparenței poate fi considerată un alt factor de risc în implementarea soluțiilor cloud, pentru că nu asigură un nivel corespunzător de înțelegere a interdependențelor dintre componentele unei implementări complexe (Mather, Kumaraswamy, & Latif, 2009).

Protecția perimetrului fizic este o cerință concretă de securitate pentru locația clientului care folosește serviciile de cloud. În același timp este un criteriu de selecție a furnizorului de cloud, care trebuie să ofere posibilitatea de acces la aceleași date dintr-o locație secundară sau mai multe. Mecanismele de diminuare a riscurilor împotriva atacurilor fizice pun pe prim plan strategiile de realizare și gestionare a copiilor de siguranță a datelor.

Neîncrederea este uneori directă cu nevoia de intimitate a datelor pe care o au numite companii în legătură cu datele pe care le stochează și prelucrează în



cloud. Chiar dacă în cele mai multe materiale, intimitatea este tratată în categoria confidențialității, termenul de intimitate este mult mai potrivit în contextul manipulării datelor cu caracter personal. Scepticii cloud-ului sunt de părere că marii furnizori de cloud sau alte servicii din web-ul social folosesc în scopuri de afaceri datele personale ale angajaților și oamenilor în general. O simplă căutare pe oricare motor de căutare vă va oferi publicitate contextuală în oricare alt site. Motivul este unul profesionist de canalizare a mesajelor publicitare pe nevoile reale ale unui individ. Dar, cum ar putea face furnizorii acest lucru fără stocarea unei cantități de date, fie și infimă, care poate determina un profil temporar sau pe termen îndelungat al unui utilizator al Internetului; pentru a determina vulnerabilitățile unui sistem cloud trebuie să ținem seama de o serie de factori diferențiatori față de implementările locale (Hugos & Hulitzky, 2011):

- Intern versus Extern – cu referire la locația de stocare a datelor o Deschis versus Proprietar – cu referire la forma de proprietate a echipamentelor de prelucrare și stocare și modului de acces la resursele respective;
- Externalizat versus internalizat – cu referire la modul în care se asigură suportul pentru serviciile puse la dispoziție;
- În perimetrul de securitate versus în afara perimetrului – cu referire la modelul clasic de securizare a infrastructurii de rețea locale prin intermediul dispozitivelor de tip firewall.

Fiecare clasă de controale are propriile sale categorii de riscuri și vulnerabilități specifice aplicabile la nivel general sistemelor informaționale, inclusiv arhitecturilor cloud. Principalele vulnerabilități la care se expun



companiile sau indivizii în momentul accesului la tehnologiile cloud sunt prezentate succint în paragrafele următoare.

Vulnerabilități ale clienților de conectare în cloud

Având în vedere că metodele de conectare la serviciile cloud includ browser-e și aplicații specifice, clienții trebuie să se asigure că acestea sunt protejate și securizate. Una din cele mai comune probleme legate de browser-e este aceea a instalării add-on-urilor de tip adware care pot colecta datele de conectare ale utilizatorilor, în felul acesta expunând întreaga companie la riscuri de acces neautorizat la conținutul informațional stocat în cloud. Salvarea parolelor în browser-e sau aplicații poate constitui un alt risc în cazul pierderii sau furtului dispozitivului de acces. Pentru diminuarea riscurilor companiile folosesc metode specifice de securizare a browser-elor și aplicațiilor. Dintre acestea cele mai întâlnite sunt: localizarea geografică a unui dispozitiv, ștergerea de la distanță a conținutului stocat, blocarea dispozitivului sau implementarea mecanismelor de dublă autentificare: nume de utilizator + parolă și un cod temporar generat de o aplicație specifică.

Criptarea datelor și comunicațiilor

Fiecare serviciu de cloud transferă datele prin intermediul canalelor securizate: HTTPS, SSH, RDP, FTPS, dar revine în sarcina clientului să se asigure în momentul conectării că accesează site-ul corect pentru autentificare. Phishing-ul a ajuns o tehnică destul de elaborată în redirectarea utilizatorilor către site-uri care emulează cât mai fidel site-urile originale, reușind astfel să intre în posesia datelor de autentificare ale utilizatorilor. Majoritatea browser-elor moderne au mecanisme de protecție a phishing-ului prin validarea certificatelor și criptarea a comunicației dintre client și serviciul



cloud. Un alt risc legat de certificatele digitale și criptarea comunicațiilor și datelor este reprezentat de scurgerea de informații din cadrul companiei și repudierea³⁸ conținutului informațional. Mecanismele de tipul managementul drepturilor digitale (DRM- – Digital Rights Management) și mecanismele privind prevenirea scurgerii informațiilor (DLP- Data Loss Prevention) sunt din ce în ce mai utilizate atât în interiorul companiilor cât și în cloud, furnizorii punând la dispoziție servicii DRM integrate cu mecanismele de autentificare și identificare a utilizatorilor. Din cele mai frecvente măsuri implementate în DRM amintim: semnarea conținutului informațional, criptarea conținutului informațional, protecția asupra anumitor operațiuni comune precum copierea, redistribuirea, și mecanisme complete de expirare a conținutului informațional după o anumită perioadă de timp. DRM asigură în același timp mecanisme concrete de protecție de tipul FYEO- For Your Eyes Only – Exclusiv doar pentru ochii tăi asigurându-se astfel că numai destinatarul unui mesaj este capabil să îl deschidă și citească.

Microsoft Azure

Este o platformă cloud privată și publică care ajută dezvoltatorii și profesioniștii IT să construiască implementarea și gestionarea aplicațiilor. Utilizează tehnologia cunoscută sub numele de virtualizare. Virtualizarea separă cuplarea strânsă dintre hardware și sistemul de operare folosind un strat de abstractizare numit hypervisor. Hypervisor emulează toate funcțiile unui computer dintr-o mașină virtuală, poate rula mai multe mașini virtuale în același timp și fiecare mașină virtuală poate rula orice sistem de operare, cum ar fi Windows sau Linux.



Azure preia această tehnică de virtualizare și o repetă la scară masivă în centrul de date deținut de Microsoft. Fiecare centru de date are multe rafturi pline cu servere și fiecare server include un hypervisor pentru a rula mai multe mașini virtuale. Comutatorul de rețea oferă conectivitate la toate acele servere.

Instrumentele, template-urile preconstruite și serviciile gestionate de Azure ajută la construcția și administrarea rapidă a aplicațiilor enterprise, mobile, web și IoT (Internet of Things). Sistemul a fost conceput pentru a crea, distribui și upgrada aplicații web fără ca utilizatorii să mai fie nevoiți să apeleze sau să mențină resurse foarte scumpe. Hosting-ul și gestionarea mediului se realizează și se menține la centrele Microsoft Data. Fiind un serviciu de cloud computing, Azure funcționează similar cu serviciile Amazon Web Services (AWS) și Google Cloud Platform.

Microsoft a dezvăluit Windows Azure la începutul lunii octombrie 2008, dar a intrat în funcțiune după februarie 2010. Mai târziu, în 2014, Microsoft și-a schimbat numele din Windows Azure în Microsoft Azure. Azure a oferit o platformă de servicii pentru serviciile .NET, Serviciile SQL și multe Servicii Live. Mulți oameni erau încă foarte sceptici cu privire la „nor”. Ca industrie, intram într-o lume nouă, curajoasă, cu multe posibilități. Microsoft Azure devine din ce în ce mai mare și mai bun în zilele următoare.

Sunt adăugate mai multe instrumente și mai multe funcționalități. Are două lansări de acum. Este o versiune celebră a Microsoft Azure v1 și mai târziu Microsoft Azure v2. Microsoft Azure v1 a fost mai mult bazat pe scripturi JSON decât noua versiune v2, care are interfață de utilizare



interactivă pentru simplificare și învățare ușoară. Microsoft Azure v2 este încă în versiunea de previzualizare.

Azure ne poate ajuta afacerea în următoarele moduri:

- Capital mai puțin: nu trebuie să ne facem griji cu privire la capital, deoarece Azure reduce costul ridicat al hardware-ului. Pur și simplu plătiți pe măsură ce mergeți și vă bucurați de un model bazat pe abonament, care este bun cu fluxul dvs. de numerar. De asemenea, configurarea unui cont Azure este foarte ușoară. Pur și simplu vă înregistrați în Azure Portal și selectați abonamentul necesar și începeți.
- Cost operațional mai mic: Azure are un cost operațional scăzut, deoarece rulează pe serverele sale a căror singură sarcină este să facă cloud-ul funcțional și fără erori, de obicei este mult mai fiabil decât propriul server la locație.
- Eficient din punct de vedere al costurilor: dacă instalăm un server pe cont propriu, trebuie să angajăm o echipă de asistență tehnică care să le monitorizeze și să ne asigurăm că lucrurile funcționează bine. De asemenea, ar putea exista o situație în care echipa de asistență tehnică durează prea mult timp pentru a rezolva problema apărută pe server. Deci, în acest sens, este mult prea prietenos cu buzunarul.
- Opțiuni ușoare de backup și recuperare: Azure păstrează copii de siguranță ale tuturor datelor dvs. valoroase. În situații de dezastru, vă puteți recupera toate datele cu un singur clic fără ca afacerea dvs. să fie afectată. Soluțiile de backup și recuperare bazate pe cloud economisesc timp, evită investițiile inițiale mari și acumulează expertiza terță parte ca parte a tranzacției.



- Ușor de implementat: este foarte ușor să implementați modelele dvs. de afaceri în Azure. Cu câteva activități prin clic, ești gata. Chiar și există mai multe tutoriale pentru a vă face să învățați și să implementați mai rapid.
- Securitate mai bună: Azure oferă mai multă securitate decât serverele locale. Fiți fără griji în privința datelor dumneavoastră critice și a aplicațiilor de afaceri. Deoarece rămâne în siguranță în Azure Cloud. Chiar și în dezastrele naturale, unde resursele pot fi afectate, Azure este o salvare. Norul este mereu pornit.
- Lucrați de oriunde: Azure vă oferă libertatea de a lucra de oriunde și de oriunde. Necesită doar o conexiune la rețea și acreditări. Și cu cele mai serioase servicii cloud Azure care oferă aplicații mobile, nu ești limitat la dispozitivul pe care îl ai la îndemână.

Colaborare sporită: cu Azure, echipele pot accesa, edita și partaja documente oricând, de oriunde. Ei pot lucra și atinge obiectivele viitoare mâna în mâna. Un alt avantaj al Azure este că păstrează înregistrări ale activității și datelor. Marcajele de timp sunt un exemplu de păstrare a evidențelor Azure. Marcajele de timp îmbunătățesc colaborarea în echipă prin stabilirea transparenței și creșterea responsabilității.

În mod tradițional, companiile și organizațiile de orice fel ar găzdui propria infrastructura utilizând propriul server web pe propriul hardware. Acestea ar trebui să aibă personal care să se ocupe de gestionarea tehnologiei, o conexiune solidă la internet sau mai mult hardware de server pentru mai multă putere, iar toate acestea generează cheltuieli semnificative. Cloud computing presupune ca organizațiile să plătească doar accesul la o cantitate însemnată de resurse de calcul furnizate de Microsoft, decât să folosească propriul echipament.



Tehnologia Azure oferă un director cu sute de servicii diferite pe care le poți utiliza, inclusiv baze de date, copii de rezerva, servere de email, mașini virtuale complete, stocare de fișiere, directoare de utilizatori, servicii pentru aplicații mobile și web. Microsoft Azure oferă o modalitate de a utiliza resurse de calcul la distanță și este un serviciu adecvat pentru companii, organizații și chiar persoane fizice.

Serviciile oferite de Microsoft Azure:

- **Calcul:** include mașini virtuale, seturi de mașini virtuale, funcții pentru calcul fără server, lot pentru încărcături de lucru în lot containerizate, Service Fabric pentru microservicii și orchestrarea containerelor și servicii cloud pentru crearea de aplicații și API-uri bazate pe cloud.
- **Rețea:** Cu Azure, puteți utiliza o varietate de instrumente de rețea, cum ar fi rețeaua virtuală, care se poate conecta la centre de date locale; Load Balancer; Gateway de aplicație; Gateway VPN; Azure DNS pentru găzduire de domenii, Content Delivery Network, Traffic Manager, ExpressRoute dedicat conexiuni de rețea privată prin fibră; și monitorizarea și diagnosticarea Network Watcher
- **Stocare:** Include stocare blob, coadă, fișiere și pe disc, precum și un depozit de date Lake, backup și recuperare site, printre altele.
- **Web + Mobile:** Crearea de aplicații Web + Mobile este foarte ușoară, deoarece include mai multe servicii pentru construirea și implementarea aplicațiilor.



- **Containere:** Azure are o proprietate care include Container Service, care acceptă Kubernetes , DC/OS sau Docker Swarm și Container Registry, precum și instrumente pentru microservicii.
- **Baze de date:** Azure a inclus și câteva baze de date bazate pe SQL și instrumente aferente.
- **Date + Analytics:** Azure are câteva instrumente de date mari, cum ar fi HDInsight pentru clusterelor Hadoop Spark, R Server, HBase și Storm
- **Servicii AI + Cognitive:** Cu Azure dezvoltă aplicații cu capabilități de inteligență artificială, cum ar fi API-ul Computer Vision, Face API, Bing Web Search, Video Indexer și Language Understanding Intelligent.
- **Internetul lucrurilor:** include servicii IoT Hub și IoT Edge care pot fi combinate cu o varietate de servicii de învățare automată, analiză și comunicații.
- **Securitate + identitate:** Include Centrul de securitate, Azure Active Directory, Key Vault și Servicii de autentificare cu mai mulți factori .
- **Instrumente pentru dezvoltatori:** include servicii de dezvoltare în cloud precum Visual Studio Team Services, Azure DevTest Labs, implementarea și monitorizarea aplicației mobile HockeyApp, dezvoltarea mobilă multiplatformă Xamarin și multe altele.

Beneficiile Microsoft Azure



Microsoft Azure este o platformă de cloud computing care oferă următoarele tipuri de servicii:

- Infrastructura ca serviciu (IaaS)
- Platforma ca serviciu (PaaS)
- Software ca serviciu (SaaS)

Infrastructura ca serviciu (IaaS)

Mașinile virtuale, stocarea și rețelele vor intra în categoria infrastructurii ca serviciu, dar utilizatorii trebuie să facă manual construirea și implementarea aplicațiilor. Azure va suporta o gamă largă de sisteme de operare datorită Hyper-hypervisor.

Platforma ca serviciu (PaaS)

Serviciul de aplicații Azure, funcțiile Azure și aplicațiile logice sunt câteva servicii oferite de Azure în cadrul platformei ca serviciu. Acest serviciu va oferi autoscaling și echilibrare a încărcăturii și, de asemenea, va exista un mediu preconfigurat pentru aplicație.

Software ca serviciu (SaaS)

Office 365, Dynamics 365 și Azure Active Directory sunt câteva dintre serviciile oferite de Microsoft Azure în cadrul Software as a Service



(SaaS), aplicația completă va fi gestionată de Microsoft Azure, inclusiv implementarea, scalarea și echilibrarea încărcării.

Microsoft Azure își pune resursele la dispoziția companiilor și organizațiilor prin intermediul internetului. Acesta susține orice sistem de operare și o gamă largă de limbaje de programare, oferă acces la servicii integrate astfel încât utilizatorii să poată gestiona infrastructura mult mai rapid prin execuția unui număr ridicat de sarcini și prin economii financiare importante.

Azure oferă suport tehnic pentru clienți din toate regiunile globului. În România, centrul de suport tehnic beneficiază de un număr ridicat de specialiști, cei mai mulți de naționalitate română, și acoperă nivelul de suport 3 pentru majoritatea produselor cloud Microsoft. Acesta este un beneficiu major, pe care KodingTech îl folosește ori de câte ori este nevoie. De asemenea, vorbim și de suport sales/ presales cu prezență locală – canal direct de suport din partea filialelor Microsoft din România și Irlanda pentru soluții optimizate bazate pe Microsoft Azure atât din perspectiva tehnică, cât și din cea a costurilor.

Flexibilitate

Sistemul de autentificare și organizare a securității serviciilor Microsoft Azure este deosebit de flexibil și permite cea mai ușoară abordare de tip Hybrid-Cloud. Acesta poate fi utilizat fie pentru a te lega la resursele locale clasice (Windows Server), fie dacă folosești soluții hibride by design precum KodingTech K2S sau te legi la o soluție Private Cloud bazată pe VMware ori Hyper-V.



Posibilitatea rulării unei soluții locale

La nivel local, companiile și organizațiile au posibilitatea de a rula Microsoft Azure Stack pe serverele lor. KodingTech este primul partener Microsoft care a implementat o soluție Microsoft Azure Stack în România.

Funcționare neîntreruptă

Fata de alți furnizori, Microsoft Azure a fost conceput să permită accesul la toate serviciile, mașinile virtuale și aplicațiile din sistem, fără teama întreruperii. Azure este lider în domeniul performanțelor și poate oferi un acord de nivel de serviciu sau SLA de 99,95%, ceea ce înseamnă o monitorizare continuă a stării serviciilor, asistență tehnică non-stop și aproximativ 4,38 ore de oprire anual, lucru pe care majoritatea firmelor nu-l pot realiza. Microsoft Azure combină serviciul IaaS, infrastructura ca serviciu, cu PaaS, platforma ca serviciu.

Securitatea datelor

Întrucât urmează modelul standard de securitate de Detectare, Evaluare, Diagnosticare, Stabilizare și Închidere, Microsoft Azure oferă siguranța ridicată în ceea ce privește protecția datelor. Azure oferă un nivel de protecție multiplu pentru platforma și utilizatorul final prin servicii simple și ușor de folosit.

Rentabilitate

Platforma Microsoft Azure contribuie la reducerea cheltuielilor și este foarte atractivă pentru multe organizații. Mediul cloud permite organizațiilor să lanseze aplicații pentru clienți, dar și aplicații interne în cloud, lucru ce conduce la economii cu infrastructura IT și sarcini reduse de hardware. Astfel,



sunt evitate investițiile mari în achiziționarea de software sau hardware nou, iar costurile de IT pot fi alocate altor cheltuieli operaționale.

Care sunt cele mai utilizate servicii Microsoft Azure

După cum am mai menționat deja, Azure este o tehnologie de business profesională care oferă utilizatorilor acces online complet la o mulțime de servicii, aplicații și baze de date.

Obiectivul sistemului este acela de a permite companiilor să-și schimbe și să-și adapteze constant propria infrastructură IT și să simplifice managementul IT. Iată ce servicii Microsoft Azure se folosesc cel mai des:

Azure DevOPs

Este o soluție ce permite creșterea vitezei livrării proiectelor software și alegerea uzuală a echipei KodingTech. Azure DevOPs este un serviciu pe care KodingTech îl folosește pentru proiect management, pe care echipa l-a configurat by design pentru metodologia Scrum, ca o soluție de versionare de tip Git prin Azure Repos, în scopul automatizării deployment-urilor prin Azure Pipelines, pentru urmărirea vitezei, a bug-urilor sau a documentației pentru fiecare proiect.

Azure Virtual Machines

Acest serviciu este utilizat pentru a rula mașini virtuale în cloud. Reprezintă alegerea de facto în rularea aplicațiilor mobile, celor de tip e-commerce sau de tip “demanding”. La fel ca multe alte companii, KodingTech preferă mașini virtuale Linux, însă pentru aceleași proiecte se pot utiliza și arhitecturi sau “resource groups” mașini Linux și Windows. Este singurul provider mare de soluții Public Cloud ce permite ridicarea de mașini



cu licențiere de tip “bring your own licence”. Dacă ai deja o soluție de licențiere Microsoft validă, nu trebuie să mai plătești încă o dată pentru licența mașinilor din cloud.

Azure Backup

Microsoft Azure oferă servicii de backup atât pentru resursele locale cât și pentru cele din cloud. Serviciul este ușor de configurat, beneficiază de preturi avantajoase și spațiu de depozitare aproape infinit și extrem de ieftin.

Azure Managed Databases

Acest serviciu oferă implementare rapidă, scalare aproape nelimitată, performanță uriașă, plată doar a ceea ce folosești, administrare de către Microsoft, licențiere inclusă și protecție prin criptare cu chei care stau doar la utilizator sau orchestrate prin Azure Key Vault. Bazele de date cel mai des folosite de către KodingTech sunt Cosmos DB, SQL Server, MySQL și PostgreSQL.

Azure Active Directory

În cadrul acestuia identificăm trei servicii utile în administrarea proceselor de identity și security:

- Azure AD – folosit pentru autentificarea web modernă, în special pentru toate soluțiile business Microsoft (inclusiv Microsoft 365, Microsoft Azure sau Microsoft Dynamics 365);
- Azure AD Domain Services – soluția clasică de autentificare Active Directory care funcționează ca serviciu administrat de către Microsoft. Aceeași soluție poate fi administrată și de către utilizator sau KodingTech



prin sincronizarea serviciului Active Directory local cu un server de același tip și o soluție VPN care extinde reziliența serviciului în cloud-ul Microsoft;

- Azure AD External Identities – serviciu de tip SSO care permite managementul identității și autentificării pentru majoritatea aplicațiilor folosite, deoarece este ușor de integrat în toate sistemele moderne. În prezent, există deja conectori pentru mai bine de 4.000 de aplicații.

Azure Web Apps, Azure Logic Apps și Azure API Management

Toate aceste servicii sunt soluții facile pentru rularea rapidă a aplicațiilor în cloud. Sunt de mare ajutor fie că îți dorești o soluție clasică, o aplicație bazată pe microservicii sau una de tip serverless.

Azure Storage

Acest serviciu face referire la soluții de stocare de tip fișiere sau obiecte. Stocarea poate fi realizată doar în cloud, poate fi stocare hibridă, stocare pentru aplicații sau stocare pentru soluții de backup.

Azure Cognitive Services

Soluții complete pentru inteligența artificială și machine learning. Aproape orice își dorește utilizatorul poate fi livrat din Microsoft Azure: Bot Services, Computer Vision, Anomaly Detector, Cognitive Search, ML, Face Detection, Form Recognizer, Speech to Text, Text Analytics, etc. The “best” is yet to come.

Azure IoT Solutions



Microsoft Azure se diferențiază ca un provider cu foarte multe aplicații și soluții pentru scenarii de tip IoT – Internet of Things. Soluțiile principale: Azure IoT Central, Azure IoT Hub, Azure IoT Edge, Azure Stream Analytics, Azure Defender for IoT și Windows 10 IoT Core Services.

Microsoft Azure este des folosit de organizații pentru backup de date și recuperări în urma unor dezastre apărute în cadrul resurselor, însă oferă o multitudine de servicii și opțiuni. Prin intermediul acestuia poate fi accesat un set de servicii cloud profesionale orientate către diferite scenarii tehnologice, fiind o soluție excelentă de care are nevoie fiecare companie sau organizație.

Următoarele sunt câteva cazuri de utilizare pe care le-a folosit Microsoft Azure.

- Implementarea aplicațiilor: Puteți dezvolta și implementa aplicația în cloud-ul Azure utilizând serviciul numit Azure App Service și Azure Functions după implementarea aplicațiilor, utilizatorii finali îl pot accesa.
- Identity and Access Management: Aplicația și datele care sunt implementate și stocate în Microsoft Azure pot fi securizate cu ajutorul Identity and Access Management. Este folosit în mod obișnuit pentru conectarea unică, autentificarea cu mai mulți factori și guvernarea identității.
- Stocarea datelor și baze de date: puteți stoca datele în Microsoft Azure în serviciu, cum ar fi stocarea blob pentru date nestructurate, stocarea tabelului pentru date NoSQL, stocarea fișierelor și Azure SQL Database pentru baze de date relaționale. Serviciul poate fi scalat în funcție de cantitatea de date pe care o primiți.



- DevOps și Integrare continuă/Implementare continuă (CI/CD): Azure DevOps va oferi unele instrumente, cum ar fi controlul versiunilor, automatizarea versiunii, managementul lansărilor și monitorizarea aplicațiilor.

Azure pentru recuperare și backup în caz de dezastru

O gamă completă de servicii de recuperare în caz de dezastru (DR) și backup sunt disponibile de la Microsoft Azure pentru a vă proteja datele și aplicațiile vitale de întreruperi. Cu ajutorul acestor servicii, vă puteți restaura rapid datele și aplicațiile în cazul unui dezastru, replicându-le pe un site cloud secundar. Serviciile de backup Azure vă protejează, de asemenea, datele împotriva atacurilor ransomware, ștergerii neintenționate și corupției.

Cheie Azure DR și servicii de backup

- Azure Site Recovery: mașinile dvs. virtuale (VM) locale pot fi replicate mai ușor în Azure cu ajutorul acestei soluții. Puteți transfera cu ușurință mașinile virtuale (VM) la Azure în cazul unui dezastru și vă puteți menține afacerea în funcțiune. Replicarea VM Azure într-o regiune Azure alternativă este, de asemenea, acceptată de Azure Site Recovery.
- Azure Backup: Dacă doriți să protejați datele care sunt prezente în cloud, atunci trebuie să utilizați serviciul Azure Backup. Oferă o singură zonă pentru monitorizarea lucrărilor de backup, gestionarea politicilor de backup și recuperarea datelor.
- Concurență Azure

Iată câțiva dintre concurenții Microsoft Azure:



- Amazon Web Services (AWS) : lider de piață care oferă o gamă largă de servicii cloud cu o infrastructură globală extinsă.
- Google Cloud Platform (GCP): este cunoscut pentru serviciile sale inovatoare precum Big Query și TensorFlow, cu un accent puternic pe analiza datelor și învățarea automată.
- IBM Cloud: oferă o suită cuprinzătoare de servicii cloud, inclusiv soluții AI, blockchain și IoT, cu accent pe clienții enterprise.
- Oracle Cloud Infrastructure (OCI) : IT se concentrează pe soluții cloud de nivel enterprise, inclusiv baze de date, aplicații și servicii de infrastructură, valorificând expertiza Oracle în software-ul pentru întreprinderi.

Azure Cloud Shell

Azure PowerShell este o extensie a Windows PowerShell care permite utilizatorilor să gestioneze vastele caracteristici ale Azure prin interfața PowerShell. Dezvoltatorii folosesc cmdlet-uri – scripturi pre-scrise – pentru a efectua sarcini complexe precum implementarea mașinilor virtuale (VM) sau crearea de servicii cloud din linia de comandă. Azure PowerShell (APS) poate automatiza și procesele prin scripting. În timp ce unii utilizatori au observat că interfața se simte oarecum incompletă și suportul ar putea fi îmbunătățit, susținătorii subliniază simplitatea platformei în gestionarea operațiunilor de obicei dificile.

Cu Azure Cloud Shell, puteți:

- Executați comenzi și scripturi pe resursele dvs. Azure utilizând o interfață unificată de linie de comandă care oferă funcții precum completarea filelor și istoricul comenzilor.



- Gestionați-vă abonamentul Azure cu un set cuprinzător de comenzi care vă permit să creați, să enumerați și să ștergeți abonamente, precum și să controlați cheile de acces ale utilizatorilor.
- Începeți tutoriale interactive pentru a afla cum să utilizați caracteristicile comune, cum ar fi crearea de mașini virtuale sau rețele virtuale.

Acces Azure Shell

Azure Cloud Shell oferă o modalitate convenabilă de a gestiona și dezvolta resursele Azure direct din browser. Îl puteți accesa cu ușurință prin portalul web Azure sau navigând la <https://shell.azure.com>, unde puteți alege între mediile Bash și PowerShell pentru sarcinile din linia de comandă.

Azure Security

Azure Security cuprinde diversele instrumente și caracteristici oferite de Microsoft pe platforma sa Azure cloud pentru a asigura securitatea. Potrivit Microsoft, aceste instrumente includ o gamă cuprinzătoare de controale fizice, de infrastructură și operaționale concepute pentru a-și proteja serviciile cloud.

Ca platformă publică de cloud computing, Azure acceptă o gamă diversă de limbaje de programare, sisteme de operare, cadre și dispozitive. Utilizatorii pot accesa serviciile și resursele Azure de oriunde, atâta timp cât au o conexiune la internet.

Azure Security Center



Azure Security Center este o platformă cuprinzătoare de gestionare a securității oferită de Microsoft pentru utilizatorii Azure. Oferă mai multe beneficii cheie, printre care:

- **Vizibilitate și control:** le permite utilizatorilor să obțină informații și să gestioneze securitatea diferitelor resurse Azure, cum ar fi mașini virtuale, servicii cloud, rețele virtuale Azure și stocare blob.
- **Protecție pentru sarcinile de lucru hibride:** securizează încărcăturile de lucru care sunt implementate atât în medii Azure, cât și în medii non-Azure, inclusiv sistemele locale.
- **Poziție de securitate îmbunătățită:** Centrul de securitate Azure monitorizează continuu mediul cloud, ajutând utilizatorii să înțeleagă starea de securitate a resurselor lor și să își îmbunătățească postura de securitate.
- **Detectarea și reducerea amenințărilor:** Cu un tablou de bord centralizat, Azure Security Center oferă alerte și recomandări, ajutând organizațiile în detectarea și prevenirea amenințărilor la securitatea cibernetică. Acest lucru ajută, de asemenea, la respectarea reglementărilor prin eficientizarea politicilor de securitate pe platformă.

În plus, Azure Security Center abordează mai multe provocări de securitate:

- **Încărcări dinamice:** pe măsură ce clienții utilizează o varietate de servicii cloud care se schimbă frecvent, Centrul de securitate Azure simplifică implementarea standardelor de securitate și a celor mai bune practici.
- **Amenințări în evoluție:** Cu cât mai multe organizații trec la cloud public, amenințările cibernetice au devenit din ce în ce mai sofisticate. Centrul de securitate Azure ajută clienții să-și securizeze sarcinile de lucru și



minimizează vulnerabilitățile prin promovarea aderării la cele mai bune practici de securitate.

- Lipsa de expertiză în securitate: Volumul mare de alerte de securitate îi poate copleși pe administratori, în special pe cei cu experiență limitată. Azure Security Center echipează administratorii cu instrumente pentru a răspunde eficient și a gestiona aceste amenințări.

Azure Security

Azure Security- Microsoft Azure folosește un model de responsabilitate de securitate partajată, ceea ce indică faptul că securitatea este un efort de colaborare între Azure și clienții săi. În mediile locale, întreaga sarcină de securitate revine clientului. Cu toate acestea, pe măsură ce clienții trec la cloud, anumite responsabilități de securitate trec la Azure.

Responsabilități de la diferite modele de servicii cloud:

- Infrastructură ca serviciu (IaaS): Azure își asumă responsabilitatea pentru securitatea fizică, inclusiv pentru gazde, rețele și centre de date.
- Platforma ca serviciu (PaaS): Azure gestionează securitatea fizică și sistemul de operare, în timp ce responsabilitățile pentru identitatea și infrastructura directoarelor, controalele de rețea și aplicațiile sunt partajate cu clienții.
- Software ca serviciu (SaaS): Azure își asumă și mai multe responsabilități, inclusiv securitatea fizică, sistemele de operare, controalele de rețea și aplicațiile, partajând în același timp identitatea și infrastructura de directoare cu clientul.



Pe scurt, Azure securizează infrastructura fizică, dar distribuția responsabilităților variază în funcție de modelul serviciului cloud. Clienții păstrează mai multe responsabilități în IaaS în comparație cu PaaS sau SaaS. Indiferent de mediu – on-premises, IaaS, PaaS sau SaaS – clienții sunt în mod constant răspunzători pentru governanța datelor și gestionarea drepturilor, gestionarea conturilor și accesului și protecția punctelor finale.

Cele mai bune practici de securitate Azure

Azure Security servește ca o resursă valoroasă pentru recomandări de securitate și cele mai bune practici. Iată câteva sfaturi cheie pentru a vă ajuta să vă îmbunătățiți postura de securitate:

- Implementați controlul accesului bazat pe roluri (RBAC) : utilizați RBAC de la Azure Security Center pentru a gestiona permisiunile în mod eficient. Familiarizați-vă cu cele cinci roluri încorporate (Proprietar abonament, Proprietar grup de resurse, Colaborator abonament, Colaborator grup de resurse și Cititor) și două roluri de securitate specifice (Administrator de securitate și Cititor de securitate), fiecare cu niveluri diferite de acces.
- Monitorizați în mod regulat tabloul de bord Azure Security Center : urmăriți tabloul de bord pentru o vizualizare centralizată a resurselor dvs. Azure, care oferă, de asemenea, recomandări acționabile.
- Stabiliți politici de securitate : implementați politici de securitate pentru a preveni utilizarea greșită a resurselor. Azure poate genera automat o politică de securitate adaptată abonamentului dvs.



- Upgrade la Azure Security Center Standard : prin actualizarea abonamentului, puteți accesa funcții avansate, cum ar fi identificarea și rezolvarea vulnerabilităților de securitate, valorificarea analizei pentru detectarea amenințărilor și activarea răspunsurilor rapide la incidentele de securitate.
- Utilizați Azure Key Vault : stocați-vă cheile în siguranță în Azure Key Vault, care este special conceput pentru a gestiona secrete precum parolele și acreditările bazei de date.
- Implementați un paravan de protecție pentru aplicații web : protejați-vă aplicațiile de amenințările și vulnerabilitățile comune instalând un paravan de protecție pentru aplicații web.
- Activați Azure Multi-Factor Authentication (MFA) : utilizați MFA, în special pentru conturile administrative, pentru a adăuga un nivel suplimentar de securitate.
- Criptați hard disk-uri virtuale : asigurați-vă confidențialitatea datelor prin criptarea fișierelor hard disk virtuale.
- Conectați mașini virtuale Azure prin rețele virtuale : îmbunătățiți securitatea prin plasarea mașinilor virtuale Azure în rețele virtuale atunci când vă conectați la alte dispozitive din rețea.
- Utilizați protecția Azure DDoS : utilizați serviciile DDoS (Distributed Denial of Service) de la Azure pentru a proteja împotriva și a atenua atacurile DDoS.

Microsoft Azure Architecture



Microsoft Azure, o platformă binecunoscută de cloud computing, oferă utilizatorilor instrumentele necesare pentru a proiecta, implementa și gestiona numeroase aplicații și servicii. Diverse produse includ învățarea automată, dezvoltarea de aplicații mobile și soluțiile Internet of Things (IoT), făcându-l venerabil pentru aproape toate tipurile de aplicații sau servicii. Platforma Azure poate funcționa de pe computere, laptopuri, smartphone-uri și tablete și acceptă multe limbaje de programare, inclusiv HTML5, JavaScript, PHP, Python și C#.

Alături de găzduirea aplicațiilor, Microsoft Azure este, de asemenea, un loc sigur pentru a stoca informații, unde utilizatorii pot stoca fișiere online și le pot accesa de oriunde. Folosit în mod obișnuit pentru a găzdui aplicații, inclusiv e-mail și rețele sociale, poate stoca orice fel de date, de la documente la imagini la videoclipuri.

Microsoft operează, de asemenea, multe centre de date fizice la nivel global. Infrastructura IT, cum ar fi rafturile de servere și conectivitatea la rețea, este necesară pentru ca întreprinderile și organizațiile să își execute cerințele IT. Tehnica cheie în această infrastructură este virtualizarea, care reduce excesul de hardware fizic prin scalarea dinamică a resurselor necesare, în funcție de cerere. Aceasta este cheia pentru cloud computing, deoarece permite software-ului să ruleze pe orice server dintr-un centru de date.

Fundația Azure este concepută de principiile SDN. Datorită cererii din partea utilizatorilor, Microsoft a îmbunătățit continuu rețeaua Azure prin instalarea mai multor servere noi, tehnologii de virtualizare hardware și aplicații noi. Evoluția continuă a unor astfel de servicii necesită o îmbunătățire constantă a hardware-ului și software-ului rețelei deja



implementate, afectând astfel configurația și performanța întregului sistem. Acest lucru implică faptul că gestionarea unei astfel de topologii complexe de rețea este din ce în ce mai importantă pentru scalarea eficientă și gestionarea resurselor.

După ce s-a pus accentul pe tehnologie și arhitectură, designul tehnic al aplicației este o progresie firească. Fiecare aplicație este autonomă, dar următoarele resurse pot ajuta în procesul de construcție:

- **Arhitecturi de referință:** Toate arhitecturile de referință sunt concepute pentru creșterea și schimbările pe care fiecare furnizor trebuie să le aibă în zilele noastre. Puteți găsi cu ușurință o arhitectură de referință care să găzduiască numărul de oameni din echipa dumneavoastră și cerințele pe care le presupune proiectul dumneavoastră. Unul dintre motivele remarcabile ale acestor arhitecturi este că ele permit utilizatorului să înceapă să construiască de unde este confortabil, având în vedere tipul de client cu care are de-a face. Fiecare arhitectură de referință include, de asemenea, detalii de implementare care sunt necesare pentru valorificarea arhitecturii. Arhitecturile recomandate sunt supuse sponsorizării vânzătorilor pentru a-și actualiza utilizarea.
- **Principii de proiectare:** este important să apreciem principiile de design care sunt inerente diferitelor perspective. De exemplu, în contextul proceselor de proiectare la nivel înalt, există principii pentru dezvoltarea politicilor care pot fi valoroase, cum ar fi principiile de proiectare bazate pe constrângeri. În schimb, principiile de proiectare bazate pe aliniere pot fi adecvate în procesele de proiectare de nivel scăzut. Aceste principii ar trebui să fie întotdeauna utilizate ca sursă de informații în cursul realizării fazei de proiectare a sistemului.



- Modele de proiectare: Modelele de design cloud reprezintă soluții pe care furnizorii de cloud le folosesc pentru a spori fiabilitatea și sociabilitatea serviciilor lor. Aceste modele constau în cele mai bune practici, linii directoare și reguli care încapsulează strategii eficiente pentru proiectarea sistemelor cloud. Prin valorificarea acestor modele, puteți crea o arhitectură cloud mai robustă și mai eficientă.

Google Workspace

Reprezintă o suită de instrumente și aplicații cloud de colaborare și productivitate, Workspace a fost conceput pentru a fi folosit de companii de toate dimensiunile. Cuprinde numeroase aplicații Google cunoscute cum ar fi Gmail, Calendar, Drive, Meet sau Docs într-o versiune gândită special pentru a acomoda nevoie de business. Practic, aceste aplicații acoperă toate nevoile unei companii de a comunica, colabora și gestiona mai eficient sarcini în era digitală.

De la aplicațiile sale de bază cum ar fi Gmail sau Google Drive și până la funcțiile avansate, Google Workspace include instrumente inteligent integrate unul în fluxul de lucru al altuia pentru a susține munca fără întreruperi, scurtături inteligente și timp recâștigat pentru sarcinile care chiar contează.



Gmail: Un email de companie sub forma nume.prenume@companie.ro, fără reclame și mesaje spam, organizat eficient sub o interfață familiară celor mai mulți angajați/

Google Drive: Spațiu de stocare individual pentru fiecare utilizator și partajat pentru echipe, o soluție bazată pe cloud care permite accesare și colaborarea concomitentă și în timp real pe documente și prezentări.

Docs, Slides și Sheets: Aplicații cu care să creați, editați și colaborați în timp real pe documente, eliminând sesiunile multiple de feedback pe diferitele versiuni ale acestora.

Google Meet: Găzduiți cu ușurință întâlniri virtuale, videoconferințe și seminarii web, integrate perfect în Calendar și Gmail.

Google Calendar: Un calendar dinamic care se integrează perfect cu celelalte aplicații Workspace.

Google Chat: Un instrument pentru conversații care va găzdui de la discuții 1:1 și până la spații cu sute de persoane, perfecte pentru comunicarea corporate.

Fiind o platformă de aplicații bazate pe cloud, Workspace și aplicațiile sale sunt accesibile de pe orice dispozitiv care se poate conecta la Internet.

- De pe un browser modern, precum Chrome. Folosirea acestuia este o alegere standard pentru companiile care folosesc Workspace pe laptopuri și PC-uri. Angajații își pot conecta cu adresa de e-mail browserul astfel încât să poată face ușor tranziția de la o aplicație Workspace la alta. Browserul Chrome nu numai că vă oferă acces la aplicațiile Workspace, dar vă permite și să utilizați anumite funcții dezvoltate special pentru Chrome, cum ar fi



munca offline. Imaginați-vă ce util poate fi ca angajații voștri să poată folosi aplicațiile și fără conexiune la Internet. Aplicațiile se actualizează apoi odată cu conexiunea online.

- Prin aplicațiile mobile de Android și iOS. Mare parte din aplicațiile Workspace sunt disponibile și în varianta mobilă. Spre exemplu, Gmail, Calendar, Drive, Docs, Sheets, Slides, Meet, Chat și Keep pot fi descărcate și instalate fie din Google Play (Android) fie din iOS App Store (Apple).
- Prin dispozitive hardware Chrome Enterprise. Multe organizații care folosesc Google Workspace aleg să achiziționeze și dispozitive hard precum Chromebookuri, hardware Google Meet, dispozitive Jamboard sau echipamente telefonice Google Voice. Acestea se pot conecta identic cu un cont Google Workspace pentru a putea fi utilizate intern în companie.