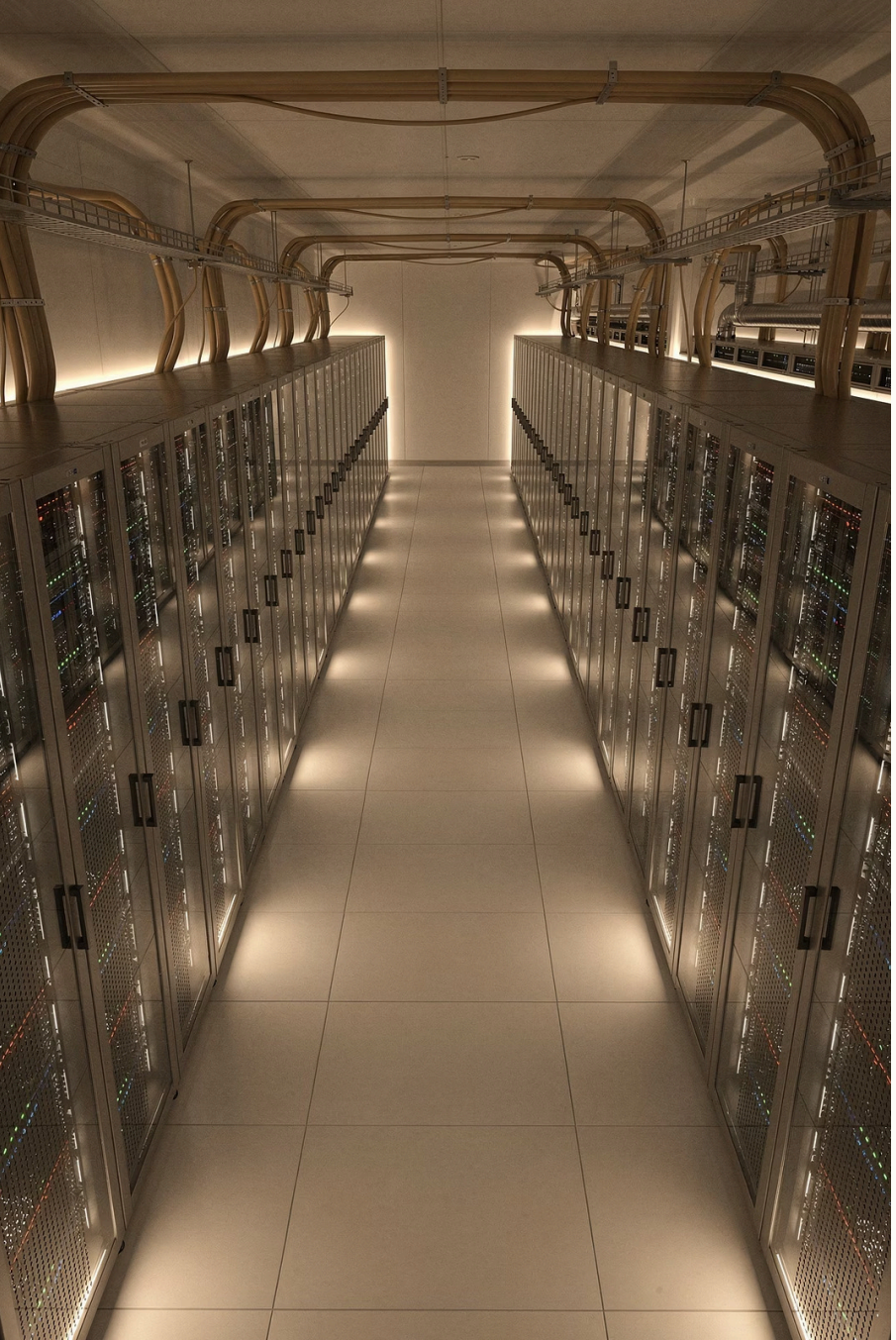
Securitate în Cloud

AZURE FUNDAMENTALS — SESIUNEA 10

Nu despre servicii. Despre **mentalitate**. Despre cum gândesc profesioniștii responsabili, despre greșelile care distrug cariere, și despre cum vă diferențiați de la prima zi.



Realitatea Incidentelor de Securitate

Credeți că hackerii atacă doar companii mari? Băncile, guvernele, corporațiile cu miliarde de euro cifră de afaceri? **Răspunsul este nu.**

Atacurile automate nu discriminează

Boți care scanează constant internetul la scară masivă verifică milioane de adrese IP simultan — porturi deschise, credențiale default, vulnerabilități cunoscute.

Un exemplu real

Un server de test creat de un junior, uitat online trei săptămâni cu parola default și portul 3389 deschis la Any. Log-urile arătau **zeci de mii de tentative** din 23 de țări diferite. Salvat doar de noroc.

70–90% din incidentele de securitate implică o eroare umană undeva în lanț. Securitatea este în mare măsură în mâinile voastre.

Ce Este Securitatea cu Adevărat?

PARTEA 1

Securitatea nu este un feature pe care îl activezi la final. Nu este un checkbox înainte de lansarea în producție. Este o **mentalitate** — un mod de a gândi fiecare decizie tehnică.

La fiecare configurație

Când setați un NSG, când alegeți o parolă, când configurați un container Blob — gândiți la securitate.

Analogia ușii deschise

Un server cu portul RDP deschis la oricine este ca o casă cu ușa larg deschisă pe cea mai aglomerată autostradă din lume — miliarde de vehicule trec în fiecare oră.

Un comportament, nu un departament

Securitatea nu aparține exclusiv echipei de securitate sau CISO-ului. Fiecare decizie a fiecărui inginer contează.

Least Privilege — Accesul Minim Necesar

PARTEA 2

Orice utilizator, serviciu sau proces ar trebui să aibă **exact atâtea permisiuni câte are nevoie** pentru a-și îndeplini rolul. Nimic mai mult. Sună simplu. În practică, este ignorat constant.

Scenariul clasic

Un junior primește rol de **Owner** pe subscripția principală. Câteva săptămâni mai târziu, confundă un Resource Group de test cu cel de producție și apasă Delete. Baza de date principală, storage-ul aplicației, configurațiile critice — dispărute în câteva secunde. Zile de recuperat, dacă există backup-uri.

Dacă juniorul ar fi avut **Contributor doar pe Resource Group-ul de test**, eroarea ar fi fost imposibilă.

Roluri RBAC în Azure

Reader

Poate vedea resurse, nu le poate modifica

Contributor

Poate crea și modifica, nu poate gestiona accesul

Owner

Control complet — acordați cu extremă atenție

Regula practică: acordați rolul cel mai restrictiv care permite îndeplinirea sarcinii. Least Privilege se aplică și serviciilor — o aplicație accesează doar containerul specific pe care îl folosește, nu întregul Storage Account.

Parole, MFA și Identitate

PARTEA 3

Câte conturi online aveți? La câte folosiți aceeași parolă? Dacă răspunsul nu este zero — aveți o problemă de securitate personală care se poate replica în viața profesională.

Credential Stuffing

Atacatorii testează automat miliarde de perechi email+parolă din breșe anterioare pe sute de servicii. Dacă reutilizați parole, sunteți vulnerabili.

Password Manager

Parole unice și complexe pentru fiecare cont. Memorați o singură parolă master. Soluții excelente, unele gratuite.

MFA — Al doilea factor

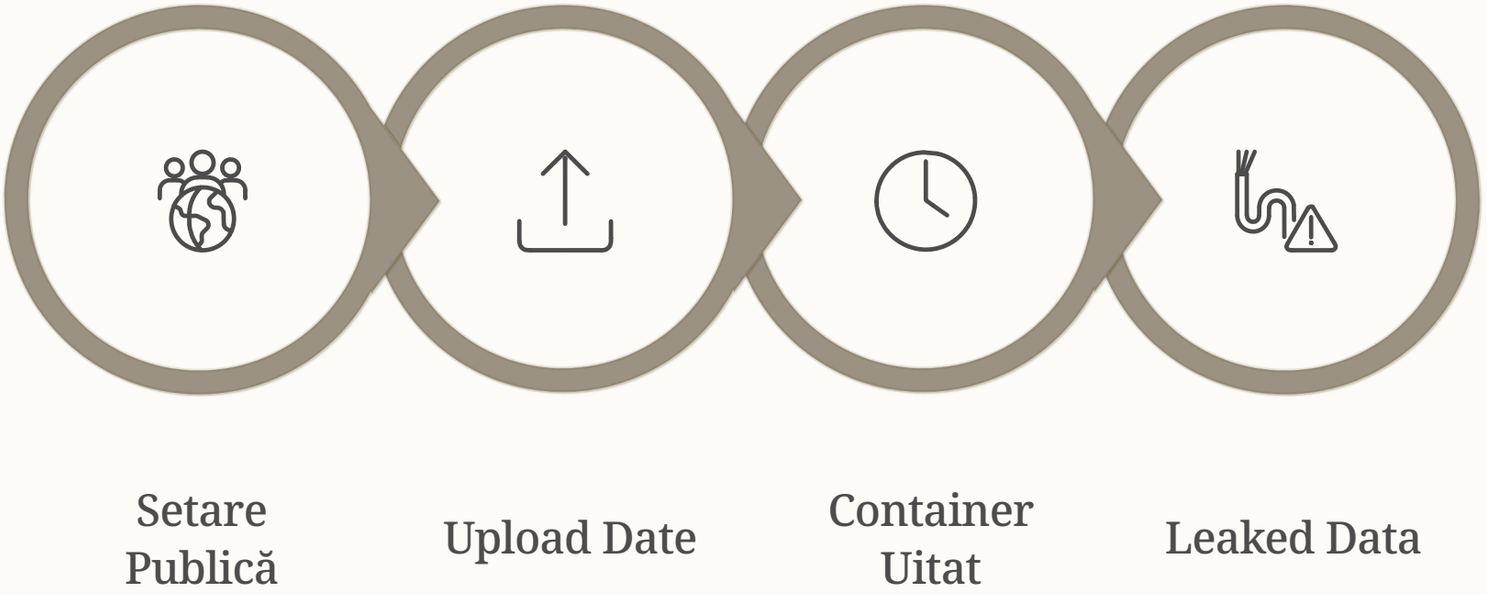
Ca o alarmă adăugată la cheie. Chiar dacă parola este compromisă, atacatorul nu poate intra fără telefonul vostru fizic.

Conturile cu MFA activat sunt **de peste 99%** mai puțin susceptibile la compromitere prin credential stuffing sau brute force. Pe conturile cloud de producție: MFA nu este opțional — este **obligatoriu**.

Public vs. Private — Consecințele Neglijenței

PARTEA 3 — CONTINUARE

Vă amintiți exercițiul cu container-ul Blob setat Public? Iată ce se întâmplă când această greșeală se face cu date reale ale clienților.



Consecințele GDPR

- Notificarea tuturor clienților afectați
- Investigație externă de cybersecurity
- Amenzi: până la 4% din cifra de afaceri globală sau 20M euro
- Pierderea reputației și a clienților

Regula de aur

Dacă nu ai un motiv **explicit, documentat și aprobat** să faci ceva public — lasă-l privat.

Defaultul în cloud trebuie să fie restrictiv. Deschizi accesul când ai nevoie, nu îl închizi după ce ai terminat.

Nu sunteți concediați pentru că nu știți. Sunteți concediați pentru neglijență.

GDPR și Responsabilitatea Legală

CADRU LEGAL

GDPR nu este o problemă abstractă a departamentului juridic. Are implicații directe pentru **arhitectura cloud pe care o construiți**.

Localizarea datelor

Datele personale ale cetățenilor europeni trebuie stocate în regiuni geografice aprobate. Nu mutați arbitrar date pe servere din SUA sau Asia fără consimțământ explicit și mecanisme juridice adecvate.

Least Privilege aplicat datelor

Accesul la date personale trebuie limitat strict la persoanele cu nevoie legitimă. Același principiu, aplicat acum la nivel de date, nu doar de resurse cloud.

Criptare și raportare

Datele sensibile trebuie criptate în tranzit și în repaus. Breșele care afectează date personale trebuie raportate autorităților **în 72 de ore**.

Când nu știți dacă o decizie tehnică are implicații de conformitate — **întrebați. Escaladați. Nu presupuneți că este în regulă.**

Backup Nu Este Opțional

PARTEA 5

Dacă astăzi, în acest moment, baza de date principală a companiei ar fi ștearsă accidental — **cât de curând ar putea fi recuperată? Ce date ați pierde?** Dacă nu știți răspunsul, aceasta este o problemă.

01

Există backup?

Nu presupuneți că există. Verificați explicit. Un senior care configurează producție fără backup are o lipsă gravă de profesionalism.

02

Backup-ul funcționează?

Un backup care nu poate fi restaurat nu este un backup — este o iluzie de siguranță. **Testați restaurarea periodic.**

03

Cât de recent este?

Dacă backup-ul este de ieri și sistemul a procesat 10.000 de tranzacții astăzi, acele tranzacții nu sunt în backup. Calculați RPO-ul real.

În Azure, serviciile managed — Azure SQL Database, Blob Storage cu versioning, Azure Backup — oferă backup automat. Dar **automat nu înseamnă configurat**. Verificați că backup-urile sunt activate și că retenția este suficientă.

PAUZĂ

10 minute

Revenim cu **Assume Breach** — cel mai important concept din securitatea modernă — și cu greșelile clasice ale juniorilor în cloud.

Assume Breach — Gândește că Vei Fi Atacat

PARTEA 6

Modelul tradițional: **castelul și șanțul**. Perimetru puternic, ziduri înalte. Dacă nimeni nu trece, ești sigur. Problema: presupune că perimetrul poate fi perfect. Nu poate.

Perimetrul poate fi depășit prin:

- Email de phishing care instalează malware pe laptopul unui angajat
- Credențiale compromise ale unui utilizator
- Vulnerabilitate zero-day fără patch disponibil
- Furnizor terț cu acces la sistemele voastre, compromis

Assume Breach în practică

- **Least Privilege** — daunele sunt limitate la ce poate accesa contul compromis
- **Segregarea rețelei** — subnets separate, NSG-uri între componente
- **Monitorizare activă** — log-urile detectează activitatea suspectă rapid
- **Backup și recuperare** — chiar dacă cel mai rău scenariu se materializează

Nu vă cer să implementați Zero Trust complet astăzi. Vă cer **mentalitatea**: niciodată nu presupuneți că ceva este sigur pentru că este în interiorul unui perimetru.

Greșelile Clasice ale Juniorilor în Cloud

PARTEA 7

Nu ca să vă judec — ci ca să le recunoașteți, să le evitați, și să interveniți constructiv când le vedeți la alții.

1

Deschid tot ca să meargă

Portul la Any, permisiuni maxime, resursa publică. Funcționează. Dar problema nu a fost rezolvată — a fost ascunsă. **Înțelegeți de ce e blocat înainte să deschideți.**

2

Copiază fără să înțeleagă

Tutorialele au adesea configurații insecure intenționate pentru simplitate. **Citiți și înțelegeți ce faceți înainte să executați.**

3

Commit credențiale pe GitHub

Roboți scanează constant GitHub pentru chei API și parole. Dacă se întâmplă: **nu ștergeți commit-ul — rotați imediat credențialele.**

4

Ignoră alertele

O alertă ignorată este o problemă netratată. **Orice alertă se urmărește până la rezolvare sau concluzie documentată.**

5

Nu șterg resursele de test

VM-uri pornite inutil, baze de date cu date de producție, costuri lunare inutile. **Orice resursă de test are o dată de expirare.**

6

Nu documentează și nu întreabă

Dacă nu e scris, nu a existat. A pune o întrebare bună este semn de profesionalism, nu de slăbiciune.

Cum Arată un Junior Bun în Cloud?

PARTEA 8

Pune întrebări și recunoaște limitele

Nu presupune că știe. Nu presupune că altcineva se ocupă. Niciun senior nu se așteaptă ca un junior să știe totul — se așteaptă să fie **cinstit**.

Respectă resursele și datele

O VM pornită costă bani reali. Datele clienților sunt o responsabilitate, nu un asset al echipei tehnice. Accesul la producție este un privilegiu.

Gândește înainte să execute

Nu copiază fără să citească explicația. Nu aplică soluții din StackOverflow fără să le înțeleagă. **Nu face deploy în producție vineri după-amiaza.**

Tratează greșelile ca oportunități

Toată lumea greșește. Diferența este în răspuns: recunoști rapid, comunici, înveți, implementezi un proces care previne repetarea.

Exercițiu Final — Cinci Scenarii

PARTEA 9

Pentru fiecare scenariu: **ce este greșit, care este riscul, și ce ar trebui făcut corect?**

#	Scenariul	Ce este greșit?	Ce ar trebui făcut?
1	VM de test cu portul RDP deschis la Any, rămasă pornită	Atac brute force în ore; VM facturată inutil	Source = My IP; VM oprită/deallocated când nu e folosită
2	Cont Azure nou fără MFA activat — "oricum nu are date sensibile"	Orice cont Azure poate crea resurse costisitoare sau distructive	MFA activat imediat, înainte de orice altceva
3	VM de development pornită non-stop pentru că "durează să pornească"	500 ore/lună de cost fără valoare	Stop Deallocate zilnic; Auto-shutdown configurat în Azure
4	Container Blob Public cu imagini de produs — cineva adaugă export cu date clienți	Date personale accesibile public; risc GDPR major	Containere separate; SAS cu expirare pentru active publice
5	Coleg primește Owner temporar în urgență, "îl schimbăm după"	Temporar = permanent în practică; acces complet la tot	Chiar și în urgență: 5 minute pentru permisiunile minime necesare

Tema pentru Acasă

REFLECȚIE ȘI CONSOLIDARE

Tema de astăzi este mai reflexivă decât cele anterioare — și asta este intenționat. Dacă regulile sunt ale voastre, le veți respecta.

5 Reguli Personale

Scrieți cinci reguli de securitate pe care le veți respecta în carieră. Nu le copiați — formulați-le cu cuvintele voastre, plecând de la ce ați auzit azi.

Least Privilege în viața reală

Explicați ce înseamnă Least Privilege folosind un exemplu concret din viața de zi cu zi — nu din IT.

De ce MFA contează

Explicați cum funcționează un atac credential stuffing și cum MFA îl oprește. Puteți folosi analogia cheie-alarmă.

Bonus: Defender for Cloud

Cercetați Microsoft Defender for Cloud. Cum evaluează postura de securitate a resurselor Azure? Cum l-ați integra în workflow-ul zilnic?

Ce V-ați Transformat în Zece Sesiuni

Ați intrat cu background-uri variate. Unii știau ce este un IP, alții auzeau primul data de subnet. Acum, **nu mai sunteți începători în cloud.**

Rețele virtuale Construiți de la zero cu NSG-uri și RBAC	**Compute & Storage** VM-uri, aplicații web, date protejate
Monitorizare Sisteme monitorizate, alerte și reacții	**Mentalitate** Gândiți responsabil din perspectiva securității

> Sesiunea finală — nr. 12 — integrează tot: rețea, securitate, compute, storage, baze de date, monitorizare. Veți construi o arhitectură reală și vom vorbi despre certificările Azure, cariera în cloud și pașii concreți următori.

Tehnica se poate învăța din documentație. **Mentalitatea se formează prin experiență, reflecție, și conversații ca aceasta.** Ați făcut astăzi un pas important spre a deveni nu doar tehnicieni cloud, ci **profesioniști cloud responsabili.**

Vă mulțumesc. Ne vedem la sesiunea finală. 🙏