

**Digi 24 - 18.04.2022**

**Titlul: Jurnalul de seară - 22 de instituții refuză cloud-ul guvernamental**

**Realizator: Cosmin Prelipceanu**

**Invitat: Anton Rog, șeful Centrului Național Cyberint al SRI**

**"C. Prelipceanu:** Despre proiectul cloud-ului guvernamental. Știți, e problema pe care o avem cu toții - mergem la o instituție, instituția ne cere să aducem copii și hârtii de la altele. Dacă toate instituțiile acestea ar fi legate între ele și ar face schimb de informații, totul s-ar rezolva mult mai ușor. Cloud-ul guvernamental ar rezolva problemele acestea. Este finanțat prin PNRR cu aproape 500 de milioane de euro. Doar că deja întâmpină proiectul primele piedici pentru că sunt instituții care ori nu au înțeles, ori se tem, ori nu au înțeles și se tem și atunci au nevoie de explicații. Să vedem cum stau lucrurile. Există o ordonanță de guvern, există un proiect de ordonanță de guvern pentru funcționarea acestui cloud guvernamental. Ordonanța este în dezbatere publică și pentru ca proiectul să facă niște pași, niște instituții care au fost desemnate de Guvern să se ocupe de acest proiect, adică Autoritatea pentru Digitalizarea României, SRI și STS, au răspândit pe la instituțiile publice care ar trebui să participe la acest proiect, un chestionar. Trebuiau, de exemplu, instituțiile să spună ce fel de nevoi de hard au, ce fel de nevoi de soft au și așa mai departe, ca să porțeze toate datele pe care le au în sistemul acesta comun. Din 108 instituții, 22 ori nu au răspuns deloc, ori au spus că ele nu vor să facă parte din proiect, altele au spus că dau niște date, dar nu le-au dat complet. Ce e de remarcat, de exemplu este că dintre instituțiile acestea 22 fac parte unele extrem de importante, cum ar fi Evidența Persoanei, Pașapoartele, Permise și înmatriculări, Poliția de Frontieră, Poliția Română, Imigrările, Registrul Comerțului, Curtea Constituțională, DNA, DIICOT. Unele dintre ele, repet, au zis că nu vor să intre, altele au zis că mai au nevoie de ceva explicații, altele au zis că nici nu vor răspunde vreodată. Motiv pentru care l-am invitat în studioul Digi 24 pe Anton Rog, este șeful Centrului Național Cyberint al SRI. Bună seara!

**A. Rog:** Bună seara! Vă mulțumesc pentru invitație!

**C. Prelipceanu:** Avem nevoie de explicații. Dintre instituțiile acestea, mi s-a părut absolut remarcabil comentariul, reacția pe care a avut-o șeful Autorității Electorale Permanente, Autoritatea Electorală Permanentă fiind printre instituțiile care nu vor să intre în cloud deloc. Este un răspuns pe care l-a dat domnul Constantin Mitulețu Buică pentru Libertatea. Și sună în felul următor: 'Noi nu considerăm normal ca STS și SRI să aibă acces la toate datele și documentele pe care Autoritatea Electorală Permanentă le pregătește în vederea alegerilor. E, în primul rând, o problemă de imagine. Nu are sens să lăsăm să planeze suspiciunea că o unitate militară, oricare ar fi ea, are acces la astfel de documente'.

**A. Rog:** Dacă mă întrebați pe mine, este o ipoteză falsă.

**C. Prelipceanu:** Care dintre ele?

**A. Rog:** Aceasta a AEP și, în general, ipotezele care spun că cele două instituții ar avea acces la datele eventualelor instituții care vor migra în acest cloud. Și dacă vreți să mă refer direct la AEP, în trecut, în anii trecuți, cu ocazia mai multor alegeri, Autoritatea Electorală Permanentă s-a adresat oficial Serviciului Român de Informații, în speță Centrului Național Cyberint, pentru a-i solicita sprijin în evaluarea cibernetică a aplicațiilor folosite în alegeri. De fiecare dată Centrul i-a răspuns. În multe situații a găsit și vulnerabilități și a dat recomandări AEP-ului pe care le-a implementat și, în felul acesta, am avut alegeri corecte. Nu cred că Autoritatea atunci știa că Serviciul e cum trebuie și, dintr-o dată, a descoperit că Serviciul are acces la date. Deci ipoteza este una incorectă. Dar nu aș vrea să mă refer numai la această chestiune. Să discutăm în general. Păi, de ce nu vin unele instituții în cloud? Unele instituții nu vin în cloud pentru că au aplicații care nu sunt pregătite pentru cloud și care necesită un efort deosebit pe care nu pot să îl facă acum, dar pentru chestiunea aceasta sunt pregătiți bani în zona de migrare cu care să se facă cu piața privată. Alte instituții nu vin în cloud din motive de genul AEP care nu au niciun fundament. Din punct de vedere tehnologic, și mă refer aici numai la Serviciul Român de Informații, Centrul Național Cyberint, rolul lui este de a asigura securitatea cibernetică. De ce asigură Centrul Național Cyberint securitatea cibernetică? Pentru că cloudul guvernamental este o infrastructură critică. Dacă nici cloudul guvernamental nu este infrastructură critică atunci nimic nu mai este infrastructură critică. Afectarea cloudului guvernamental duce automat la afectarea securității naționale. Gândiți-vă că vor fi 60 de instituții care migrează și, dintr-o dată, cloudul nu mai este disponibil pe motive de securitate. E afectată toată societatea, Guvernul, economia și tot ce mai doriți. Din acest motiv, pentru că Serviciul Român de Informații este instituția care se ocupă de cunoașterea, prevenire și contracararea amenințărilor la securitatea națională, iar, dacă discutăm de contracarare în spațiul cibernetic, ea nu poate să fie decât una tehnologică, iar Serviciul o face prin unitatea sa specializată Centrul Național Cyberint. Deci toate echipamentele pe care noi le punem pe partea de securitate cibernetică nu au acces la date. Ele se uită la loguri, la jurnale și jurnalizează evenimente de securitate cibernetică, evenimente care sunt centralizate într-un sistem central, unele dintre ele ajung să fie alerte de securitate cibernetică și să fie investigate. Deci niciun fel de dată, chiar dacă am dori, dacă nu am dori, nu ajunge la noi.

**C. Prelipceanu:** Care este garanția?

**A. Rog:** Garanția este garanția tehnologică. Tehnologiile respective sunt construite pentru a nu avea acces la date, pentru a asigura numai securitate cibernetică.

**C. Prelipceanu:** Știți, oamenii ăștia, că nu e vorba doar despre AEP, oamenii aceștia care vă confruntă pe dumneavoastră în legătură cu cloud-ul guvernamental spun așa: domnule, este imposibil să ne păzească, dar să rămână la poartă! Sigur vor intra!

**A. Rog:** Dați-mi voie să vă dau un exemplu foarte clar. Noi operăm un Security Operating Center, un SOC - îi spunem Țițeica, e vestit, îl știe toată România. A fost făcut din fonduri europene în 2015. El funcționează de șapte ani. În acel SOC făcut din fonduri europene noi oferim servicii de securitate cibernetică pentru 61 de instituții din tot Guvernul României. Vă aduc la cunoștință că, în șapte ani, nu a existat nici măcar o plângere că un bit dintr-un mail, dintr-un fișier sau din ce vreți dumneavoastră a fost accesat de Serviciul Român de Informații. Și vă mai aduc la cunoștință un lucru, că, în acești șapte ani, au fost numeroase, zeci, poate sute de incidente cibernetice majore și, de fiecare dată, știți cui s-au adresat instituțiile respective? Serviciului Român de Informații, invariabil!

**C. Prelipceanu:** Dar au știut că există aceste pericole sau v-ați ocupat de ele înainte?

**A. Rog:** Au știut că există. A fost și un moment de inflexiune, când perioada de viață a proiectului, de cinci ani, care s-a terminat în octombrie 2020, n-a mai fost finanțat din fonduri europene și a fost o perioadă de o lună sau de două luni în care unele instituții au înțeles pe echipamentele în custodie să își prelungească licențele și altele, nu. Ce să vedeți, la instituțiile care nu și-au prelungit, dintr-odată toate atacurile care erau oprite de tehnologie și de noi au intrat în plin și au zis: suntem atacați cibernetic! În fapt, nu erau atacați cibernetic, efortul nostru conjugat și tehnologia nu au mai lucrat.

**C. Prelipceanu:** Cine verifică că dumneavoastră nu intrați în date?

**A. Rog:** Instituțiile respective! Pentru că noi avem o zonă...

**C. Prelipceanu:** Adică posesorii datelor?

**A. Rog:** Exact, exact. Noi avem o zonă centrală și, da, avem senzori care culeg evenimente de securitate cibernetică și atât. Sensorii sunt culeși în zona locală și de acolo sunt împinși. Oricând, orice instituție se poate uita în zona respectivă dacă noi luăm vreun fel de date. Și nu luăm niciun fel de date.

**C. Prelipceanu:** Și oamenii ăștia nu puteau să vă întrebe? Scandalul este... Reacțiile sunt foarte puternice, pentru că ce rezumă aici domnul Mitulețu-Buică este practic ce e în mințile multora dintre șefii instituțiilor ăstora. Am văzut, de exemplu, că, pe listă, sunt Ministerele Economiei, Muncii, Familiei...

**A. Rog:** Repet, unii nu le migrează pentru că au tehnologii foarte vechi...

**C. Prelipceanu:** Și anume că vă dau dumneavoastră toate datele și că SRI va deveni posesorul tuturor datelor românilor...

**A. Rog:** SRI este un instrument și SRI nu trebuie... Cum să vă zic, cloud-ul guvernamental nu trebuie să fie un cloud militarizat. El trebuie să fie un cloud dedicat cetățeanului, dedicat instituției și zonei civile. SRI a înțeles - și bănuiesc că și STS - că sunt doar două instrumente care au mai multă cunoaștere, au specialiști mai buni, pe care statul român îi folosește ca să își pună în aplicare cloud-ul. Puterea în cloud, decizia în cloud nu trebuie să fie nici la SRI, și nici la STS și trebuie să înțeleagă foarte bine aceste două instituții: trebuie să fie la ADR. ADR trebuie să fie cel care împarte resursele, decide accesul, alocarea și tot ce mai vreți în cloud.

**C. Prelipceanu:** Acum explicați-ne în felul următor: datele - odată cu intrarea în cloud, oamenii aștia doar fac share la datele pe care le au sau le și poartă într-un loc comun unde va exista o bază de date uriașă în care sunt toate datele românilor?

**A. Rog:** Cloud-ul guvernamental este o infrastructură de hardware și software pe mai multe nivele - nu vreau să fiu foarte tehnic, ca să fim înțeleși - în care sunt unele instituții fundamentale care nu pot lipsi din cloud pentru că, fără ele, cloud-ul nu are sens: Evidența Populației, Permise, Pașapoarte, adică cloud-ul trebuie să ajute instituțiile, dar mai important, să ajute cetățeanul, cum ați început dumneavoastră. Trebuie ca cel puțin cele 36 de evenimente de viață să fie rezolvate de acest cloud: să îmi fac buletin, să îmi fac pașaport, să fac o consultație medicală, să-mi deschid firmă, să-mi închid firmă, să-mi schimb obiect de activitate. Toate aceste date trebuie migrate în cloud. Cloud-ul sigur că e o tehnologie specifică. Migrarea asta nu se întâmplă peste noapte.

**C. Prelipceanu:** Asta înseamnă că le dau sau rămân proprietarul...?

**A. Rog:** Nu, înseamnă că le mută în cloud.

**C. Prelipceanu:** Adică nu mai sunt proprietarii lor?

**A. Rog:** Ba da, instituțiile sunt proprietarele datelor în continuare, în zona de cloud alocată pentru ele.

**C. Prelipceanu:** Este un spațiu comun.

**A. Rog:** Este un spațiu comun. Ceea ce aduce extrem de important cloud-ul este interoperabilitatea și ați menționat-o la început, din perspectiva clientului. Când toate acele baze de date, aplicații sunt într-un spațiu comun, atunci schimbul de date între ele trebuie să fie unul natural și să scutească într-o mare parte cetățeanul de plimbatul pe la ghișee și între instituții.

**C. Prelipceanu:** În proiectul de ordonanță scrie că SRI oferă și hardware, adică niște mașini. Mașinile ce fac, pe care le dați dumneavoastră?

**A. Rog:** Haideți să explicăm.

**C. Prelipceanu:** Spațiul de stocare e al SRI-ului?

**A. Rog:** Nu!

**C. Prelipceanu:** Cine dă spațiul de stocare?

**A. Rog:** STS. Infrastructura... Deci, buget de 560 de milioane, nu e aproape 500. Este 560. Din acest buget, 50 la sută este alocat licitației și zonei de infrastructură de care se va ocupa STS, 250 de milioane de euro. Pentru partea de securitate cibernetică, Serviciul Român de Informații, pentru că guvernul a decis să facă un cloud rezilient în patru noduri - noduri care sunt niște centre de date ce aparțin STS-ului...

**C. Prelipceanu:** Cloud rezilient înseamnă?

**A. Rog:** Înseamnă că dacă pică un nod, rămân celelalte trei, cetățeanul, instituțiile nu simt nimic, rămâne în picioare. Dacă pică al doilea nod, nu se întâmplă nimic, rămâne în picioare. Și tot așa, cu cât ai mai multe noduri, cu atât cloud-ul este mai rezilient. Din tot acest buget pentru cele patru cloud-uri estimarea noastră este că noi, pe partea de securitate cibernetică, vom folosi 7 la sută din acești bani, adică vreo 40 de milioane de euro. Echipamentele pe care le punem noi sunt echipamente de tip senzorial, echipamente care asigură numai protecție cibernetică, se uită la log-uri, la jurnale, nu se uită la...

**C. Prelipceanu:** Adică cine intră, cine iese...

**A. Rog:** Exact!

**C. Prelipceanu:** ...ce caută...

**A. Rog:** Nu, nu, nu! Nu ce caută! Nu! Doar cine intră, cine iese cine, dacă...

**C. Prelipceanu:** Și senzori înseamnă că există niște situații când sună alarma.

**A. Rog:** Exact, exact.

**C. Prelipceanu:** Spuneți-mi cine ne garantează nouă că STS, posesorul hardului, al spațiului de stocare, nu se înfruptă de acolo?

**A. Rog:** Iarăși e o chestiune tehnologică și partea de acces și de alocare nu trebuie să fie la STS, trebuie să fie la ADR, la instituția civilă. Noi, SRI-ul, credem că puterea - așa e normal - trebuie să migreze în totalitate către zona civilă, deci instituția care va aloca drepturi în cloud, care va aloca resurse, nu va fi STS-ul. STS-ul trebuie să fie și să înțeleagă lucrul ăsta: deși centrele de date sunt ale lor, nu este cloud-ul STS, este cloud-ul guvernamental și, în repetatele întâlniri pe care le am

avut, eu am spus fraza asta, pentru ca toată lumea să înțeleagă: deci de alocare și de drepturile în zona de cloud trebuie să se ocupe exclusiv ADR. STS și SRI trebuie să fie doar niște instrumente și atât.

**C. Prelipceanu:** Deci, dacă există o suspiciune la adresa dumneavoastră sau la adresa STS-ului, ADR-ul ar trebui să-și dezvolte un sistem de control.

**A. Rog:** Nu că trebuie să-și dezvolte, dar cloud-ul, când va fi făcut, va fi făcut deja cu acest sistem de control, care va fi la dispoziția ADR și numai la dispoziția ADR.

**C. Prelipceanu:** Nelămuririle și temerile oamenilor acestora ar trebui să fie lămurite de ADR care este posesorul acestei afaceri.

**A. Rog:** Păi, de-asta m-ați invitat, ca să explicăm aceste lucruri. ADR-ul este șeful acestei afaceri, ca să fie clar. Nu SRI, nu STS. Repet încă o dată, noi nu ne dorim un cloud militarizat. Mai mult, în acele întâlniri, noi - pentru că au existat reproșuri și din zona pieței private, în care au spus: domnule, îl faceți militarizat, noi nu mai putem să publicăm nimic. Noi, SRI-ul, în acele întâlniri - și țin să precizez lucrul acesta și este real și poate fi dovedit - am cerut două lucruri: bun, dacă cu banii aceștia finanțăm zona privată din cloud, nu finanțăm și zona publică, atunci cel puțin în OUG să lăsăm libertatea pentru viitor ca ADR să îți facă și un nod, două noduri publice, care să se interfațeze cu aceste noduri. Nodurile publice ce înseamnă? Înseamnă că acolo poate să vină să închirieze oricine servicii sau să pună oricine servicii și așa este normal.

**C. Prelipceanu:** Care să fie interconectate cu datele publice?

**A. Rog:** Care să fie interconectate la nivel de servicii cu cloud-ul, nu cu datele. Din motive de securitate.

**C. Prelipceanu:** Aceasta ar însemna că digitalizarea României nu este un monopol de stat.

**A. Rog:** Nu, nu este și nici nu trebuie să fie, e greșit.

**C. Prelipceanu:** Pentru că acesta a fost un reproșul Asociației Patronale din Software.

**A. Rog:** Și mai mult, tot noi am pus în OUG o clauză care spune așa: în zona privată a cloud-ului, orice dezvoltator de software, de servicii de cloud din România și le poate publica gratuit după ce aceste aplicații sunt verificate din punct de vedere al securității cibernetice de către ADR și SRI. N-au niciun cost, iar povestea care este? În cloud-ul privat au acces cele 'n' instituții, câte or fi ele, și cetățeanul privat, la anumite servicii care privesc evenimentele de viață. Deci, acele servicii pe care le publică dezvoltatorii de software în zona privată a cloud-ului vor putea fi consumate și plătite de cele 'n' instituții care sunt în zona privată. Asta este o compensație, pentru că nu avem încă de

la început unul-două noduri publice. ADR trebuie să se preocupe, după aceea, ca să existe și aceste noduri publice în care să dezvoltăm mult mai bine zona privată.

**C. Prelipceanu:** Bun, eu am înțeles, cred că au înțeles și telespectatorii noștri, numai că aici e vorba despre... ați spus că există o garanție a softului, o garanție a mașinii...

**A. Rog:** Absolut, absolut, verificabil oricând.

**C. Prelipceanu:** ...dar altă variantă de a le garanta celor care își aduc datele că ei sunt în siguranță acolo și că nimeni care nu trebuie nu intră în ele?

**A. Rog:** În orice sistem informatic cea mai importantă garanție este garanția tehnologică, pentru că garanția tehnologică, cum să vă spun, este un dat verificabil. Eu pot să vă garantez ca oficial în SRI că n-o să facem treaba asta, dar știți, e doar o vorbă. Garanția tehnologică este o chestiune dată, verificabilă prin auditare oricând, pe care nu poți să o manevrezi, s-o aranjezi fără să rămână urme.

**C. Prelipceanu:** Pentru că există și opțiunea, de exemplu, care ne vine tot de la oamenii care lucrează în branșă, există o frustrare aici că giganți internaționali ar fi vrut ca afacerea asta, cloud-ul românesc, de exemplu să fie unul complet privat, de ce nu, al unei entități internaționale?

**A. Rog:** Nicio țară din lumea asta nu își pune datele cele mai importante, protejate prin GDPR, că nu discutăm aici de date clasificate, într-un cloud care să aparțină altcuiva. Nicio țară din lumea asta n-a făcut așa și nu o să înceapă România. Însă România trebuie să încurajeze investițiile private de tehnologie de cloud în zona privată din România și cloud-ul guvernamental trebuie să permită interfațarea securizată la nivel de servicii cu orice fel de altfel de cloud al unui investitor care vine să investească în România. Nu o să dau acum un exemplu, ca să nu avantajez unul sau altul. Și apropo de investițiile străine, că mai e o dezbatere în presă - eu mă ocup de cyber, dar cred că e bine să spun și treaba asta. Toată lumea a reproșat faptul că SRI și SIE sunt în Comisia de evaluare a investițiilor străine din afara Uniunii Europene. Eu vă întreb așa, retoric, dacă în spatele unui fond de investiții descoperim că e un offshore cu trei oligarhi ruși, care vin și cumpără ceva strategic în România, dumneavoastră pe cine o să întrebați primul?

**C. Prelipceanu:** Toată lumea vă va răspunde că da, așa trebuie să se întâmple, că trebuie verificați, dar temerile sunt cu totul altele, temerile sunt că odată cu această verificare, veți mai pune și alte filtre.

**A. Rog:** Nu.

**C. Prelipceanu:** Care e garanția că nu le puneți?

**A. Rog:** Păi, garanția că nu le punem nu e niciuna, pentru că, cum să vă spun, ori că suntem, că nu suntem în Comisia aia, oricum ne consultau, deci, dacă plecăm de la reaua-credință, ceea ce nu e cazul, filtrele alea - în Comisie, cele două instituții nu au drept de vot, nici aviz nu au, doar sunt consultate cu privire la treaba asta și prezența lor în Comisie asigură un mai bun dialog și atât. Oricum ne-ar fi întrebat, iar, dacă plecăm de la reaua-credință că am fi vrut să punem niște filtre, nevoțând în Comisie, nu putem să influențăm. Faptul că suntem sau nu suntem acolo, oricum ne întrebau și oricum rezultatul întrebării, într-un fel sau altul, ajungea la Comisie.

**C. Prelipceanu:** Mai am o întrebare despre cloud, este ultima întrebare din seara aceasta, care-i va fi nivelul de transparență sau care e opțiunea dumneavoastră în privința nivelului de transparență?

**A. Rog:** Transparență totală!

**C. Prelipceanu:** Cine și cât să vadă din cloud ca să înțeleagă cum funcționează lucrurile?

**A. Rog:** Deci, Serviciul Român de Informații, în legătură cu partea de achiziții de care se va ocupa, în legătură cu tehnologiile, cu consultarea pieței are transparență totală. În raportul către Comisie - nu știu celelalte instituții cum au făcut, cel mai bine vorbesc despre SRI - noi am mers pe cinci verticale de securitate, ne-am consultat cu piața. La fiecare verticală, acolo unde am primit prețurile, am pus prețurile transparent în document ca să știe unii de alții cât au oferit și am pus numele companiilor la fiecare verticală de securitate, de la design până la securitatea utilizatorilor și vă anunț că la fiecare verticală am avut mai mult de 15 oferte. Deci, va exista competiție, transparență și tot ce doriți dumneavoastră. Deci opinia noastră este pentru transparență totală: financiară, acces la date și orice. Și nu vrem să fie militarizată, vrem să fie public pentru cetățean.

**C. Prelipceanu:** Vă mulțumesc! Să nu fie militarizată. Anton Rog este șeful Centrului Național Cyberint."