
# BULETIN
# CYBERINT

SEMESTRUL 2 - 2018

# Atacurile statale de tip APT

Campaniile de tip *Advanced Persistent Threat (APT)* au, de regulă, un impact semnificativ asupra securității naționale și sunt caracterizate printr-o succesiune de atacuri cibernetice, care debutează cu infectarea unei ținte de interes și pot avea următoarele obiective:

- exfiltrarea unor informații de interes cu valențe strategice
- sabotarea unor infrastructuri critice de tipul unor facilități industriale de importanță strategică, precum cele de producție și distribuție a energiei electrice.

Totodată, există posibilitatea ca atacatorii să utilizeze informațiile accesate neautorizat în derularea unor acțiuni de influențare a unor procese socio-politice, cu scopul de a genera dezechilibre la nivelul societății.

Aceste atacuri sunt derulate, în principal, de entități statale, ce vizează ținte din domeniile guvernamental, financiar - economic și industrial. Mai mult, nivelul tehnologic ridicat permite atacatorului să își mențină persistența în infrastructura compromisă pentru o perioadă îndelungată de timp (de la câteva luni până la câțiva ani), într-o manieră ce îngreunează detecția și analiza fișierelor malware utilizate.

Vectorul de infecție preferat de actorii statali este atacul de tip spear phishing[1]. Titlurile mesajelor e-mail utilizate în campanii de spear phishing sau cele ale fișierelor cu conținut malware atașate mesajelor sunt concepute special pentru a fi cât mai credibile și pentru a asigura o rată ridicată de succes în accesarea acestora de către destinatar. În funcție de țintă, titlul mesajului / fișierului poate reprezenta o invitație la un eveniment de importanță strategică, un document care urmează a fi supus dezbaterilor la nivel înalt sau chiar documente financiare - facturi, documente justificative, contabile - în cazul în care entitatea vizată este, spre exemplu, o companie privată.

*[1] Transmiterea de fișiere malware în atașamentul unor e-mail-uri, aparent legitime, concepute special pentru a viza un anumit destinatar. Această metodă poate fi utilizată și pentru a transmite fișiere malware specifice actorilor din domeniul criminalității cibernetice.*

Câteva exemple de titluri de e-mail / documente folosite în cadrul unor campanii de spear phishig:

*Save the Date - Task Force "Digital Economy" 23-24 October in Hamburg* - mesaj care pare a fi semnat de Ministerul Federal pentru Afaceri Economice și Energie din Germania;

*Conference_on_Cyber_Conflict.doc* - document care pare a fi semnat de Centrul de Excelență în Apărare Cibernetică al NATO;

*Prospects for US - North Korea Summit.doc* - document care pare a fi semnat de o entitate sud-coreeană;

*Mandiant_APT2_Report.pdf* - document care pare a fi un raport al unei firme de securitate cibernetică;

*BREAKING: Plane Crash in Laos Kills Top Government Officials* - titlul unui e-mail care pare a relata o știre de ultimă oră despre un înalt *oficial guvernamental.*

Operațiunile cibernetice ofensive de tip APT lansate de actori statali vizează atingerea unor obiective strategice ale statelor / entităților de origine și continuă să rămână cele mai importante amenințări cibernetice la adresa securității naționale a României.

De cele mai multe ori acțiunile acestora nu sunt influențate în mod direct de perioada de desfășurare a unor evenimente cu importanță strategică precum preluarea Președinției Consiliului Uniunii Europene de către România, împlinirea unui secol de la înfăptuirea Marii Uniri și poate chiar derularea unor procese electorale la nivel național.

Cu toate acestea, evenimentele care se încadrează în tipologia celor menționate anterior pot reprezenta factori favorizanți pentru intensificarea campaniilor lansate de către actorii statali.

# Cryptocurrency mining

Criptomonedele reprezintă un activ digital descentralizat și anonimizat, generarea și utilizarea lor fiind bazată pe algoritmi și metode criptografice. Ideea utilizării unor metode de plată electronică descentralizată, cunoscută sub denumirea de cryptocurrency, a apărut în anul 2008, când autorul, cunoscut în mediul online sub pseudonimul Satoshi Nakamoto, a publicat o lucrare cu privire la Bitcoin.

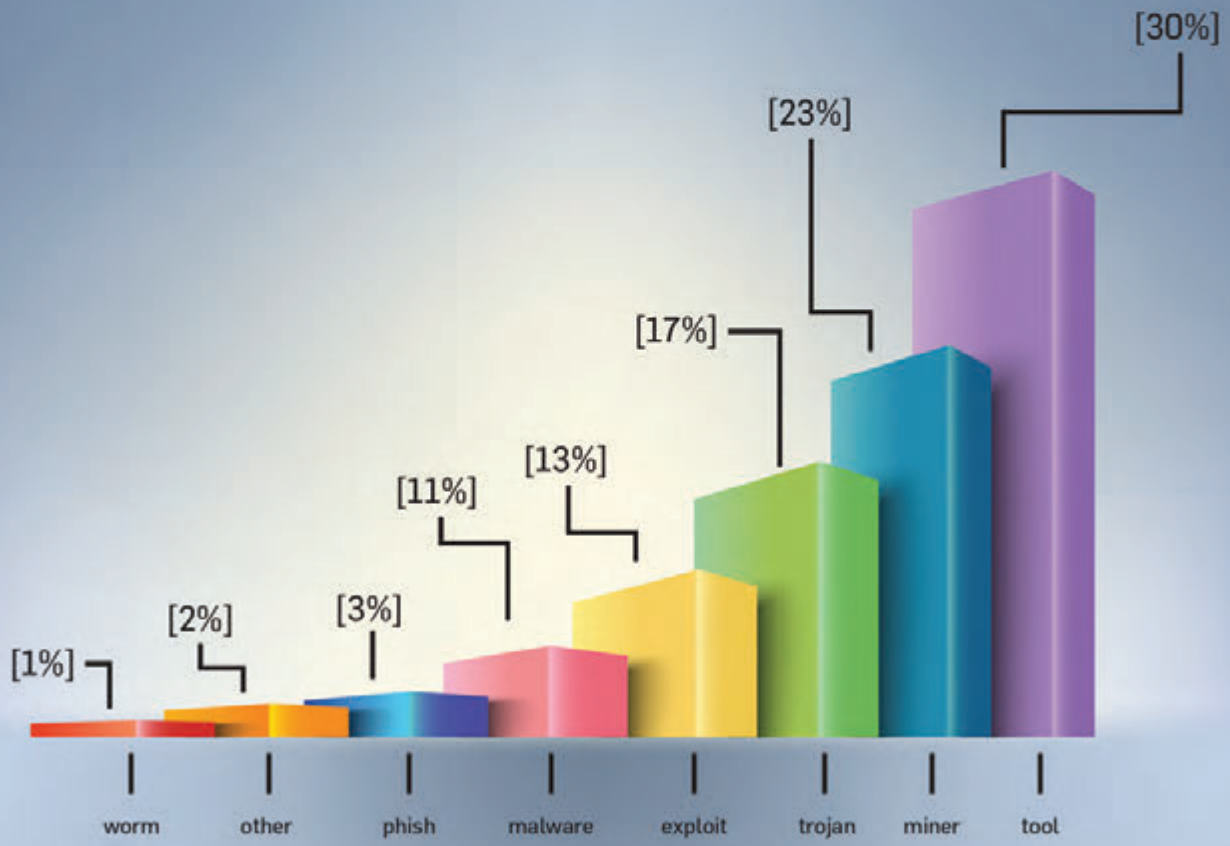
**La finalul primului semestru al anului 2018, existau peste 1600 de astfel de monede, numărul fiind în continuă creștere.**

Criptomonedele pot fi atât cumpărate, cât și create, iar procesul de creare a monedei virtuale se numește minare. Minarea se realizează prin rezolvarea unor operații matematice complexe și prin datarea și partajarea tranzacțiilor într-o bază de date publică denumită Blockchain. Operațiunea de minare este deosebit de complexă și este foarte dificil de realizat de un singur utilizator, deoarece necesită o putere de procesare foarte mare și implică, totodată, un consum ridicat de energie electrică.

**Minarea este profitabilă atât timp cât recompensele depășesc costurile de dezvoltare a unui astfel de echipament și costurile generate de consumul de energie electrică.**

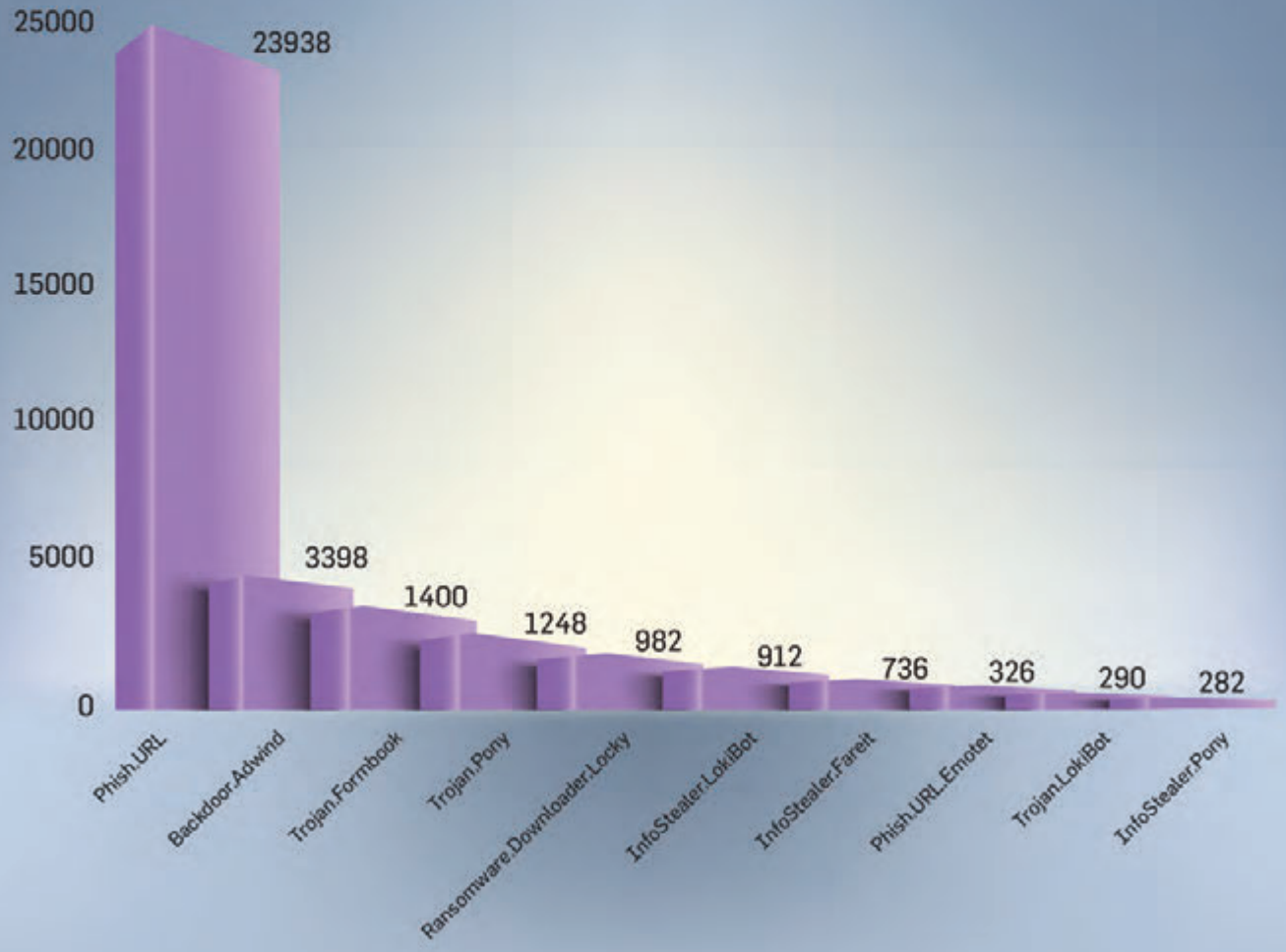
# Statistici atacuri

**Cele mai frecvente tipuri de atacuri**



# Statistici atacuri

**Top 10 campanii malware în România - Semestrul 1 din 2018**



Echipamentele utilizate în procesul de minare necesită capacități de calcul crescute și sunt denumite mineri. Astfel, s-au dezvoltat grupuri de mineri (mining pools) care combină puterea de procesare a tuturor dispozitivelor pentru rezolvarea algoritmilor producători de monede virtuale.

În prezent, cele mai răspândite metode de minare sunt **fermele de minare** sau **minarea in-browser**:

- O fermă de minare reprezintă un centru de date care conține echipamente dedicate de minare a criptomonedelor. Dimensiunea acestora poate varia de la cel puțin două echipamente dedicate, care pot fi instalate inclusiv în locuințe individuale până la câteva sute de echipamente.

- Minarea de criptomonede in-browser a devenit o metodă din ce în ce mai utilizată pentru a obține venituri prin exploatarea traficului online înregistrat pe anumite website-uri. Astfel, se utilizează puterea de calcul a dispozitivelor fiecărui utilizator care vizitează un website ce conține în codul sursă script-uri specializate pentru minare de criptomonedă.

> Un exemplu de astfel de activitate a avut loc în luna februarie, când au fost infectate cu un script de minare Monero aproximativ 4300 de website-uri care utilizau *Browsealoud - plugin folosit în cadrul site-urilor web pentru a îndeplini funcții ce facilitează accesibilitatea pentru persoanele cu handicap.*

Amenințarea cibernetică la adresa securității naționale poate fi generată prin folosirea de aplicații malware de cryptomining în cadrul infrastructurilor IT&C ale unor instituții publice. Astfel, prin infectarea cu o aplicație de acest tip, resursele hardware disponibile pe infrastructura respectivă nu mai sunt utilizate exclusiv în scopuri subsumate misiunilor instituției vizate, ceea ce poate genera îngreunarea activității acesteia, iar în final creșterea gradului de uzură a echipamentelor.

# Rezilienţa cibernetică

Atunci când utilizăm dispozitive IT&C luăm contact, conştient sau nu, cu triunghiul securităţii, care presupune menţinerea echilibrului între securitate, funcţionalitate şi optimalitate. Spre exemplu, optimalitatea crescută a unei aplicaţii poate fi obţinută inclusiv prin scăderea timpului pe care un utilizator îl petrece pentru a efectua o anumită activitate. Acest aspect poate fi realizat chiar şi prin renunţarea la o serie de politici de securitate cibernetică, cum ar fi autentificarea în minim doi factori, ceea ce poate vulnerabiliza produsul software în cauză.

Lipsa implementării acestor politici sau implementarea lor defectuoasă, dar şi nivelul scăzut de cultură de securitate cibernetică a utilizatorilor şi administratorilor potenţează apariţia unor vulnerabilităţi de securitate cibernetică care favorizează desfăşurarea unor atacuri cibernetice asupra unor infrastructuri IT&C cu valenţe critice pentru securitatea naţională. În acest context, vulnerabilităţile de securitate cibernetică pot fi clasificate în trei categorii distincte: **tehnologic, procedural şi uman.**

**Vulnerabilităţile tehnologice** sunt cele care se referă exclusiv la echipamente hardware şi produse software, fiind independente de acţiunile pe care le întreprind administratorul sau utilizatorii infrastructurii. Un exemplu în acest sens este reprezentat de uzura fizică şi morală a echipamentelor hardware şi a aplicaţiilor software existente în cadrul unei infrastructuri. Astfel, un atacator poate viza în mod special anumite echipamente pe care sunt instalate versiuni mai vechi ale unor produse software pentru care dezvoltatorul nu mai oferă update-uri de securitate.

**Vulnerabilităţile procedurale** sunt cele care se referă la existenţa politicilor de securitate şi la modul în care sunt implementate acestea într-o infrastructură IT&C. Implementarea defectuoasă a politicilor de securitate poate favoriza compromiterea acestor infrastructuri. De exemplu, administrarea şi utilizarea de la distanţă a unor aplicaţii şi echipamente, în lipsa unei conexiuni securizate, poate favoriza efectuarea de atacuri de tip *man-in-the-middle*[2], prin care poate fi interceptat traficul de reţea dintre două dispozitive.

**Vulnerabilităţile umane**, din perspectiva securităţii cibernetice, sunt cele care derivă din lipsa culturii de securitate cibernetică sau care vin ca urmare a superficialităţii de care dau dovadă atât utilizatorii, cât şi administratorii de reţea. Factorul uman se dovedeşte a fi cea mai mare sursă de erori, în condiţiile în care nu este suficient de calificat în domeniul IT&C şi nu este informat cu privire la necesitatea şi modurile de protejare a sistemelor informatice.

*[2] O formă de interceptare în care atacatorul se interpune într-un schimb de date şi are posibilitatea să acceseze conţinutul acestuia.*

În acest context se impune, diminuarea numărului și a severității vulnerabilităților de securitate cibernetică pentru a reduce frecvența și amploarea atacurilor cibernetice, dar și pentru asigurarea unui grad ridicat de reziliență a infrastructurilor IT&C cu valențe critice pentru securitatea națională. În plus, pentru atingerea acestui obiectiv, pot fi întreprinse și alte demersuri care nu depind în totalitate de aspectele de ordin tehnologic ale securității cibernetice:

- organizarea unor exerciții de securitate cibernetică la nivel național;
- crearea unei curricule pentru programe de studii universitare în domeniul securității cibernetice;
- creșterea culturii de securitate cibernetică, prin campanii de conștientizare și comunicare publică - articole și publicații de specialitate;
- crearea și dezvoltarea unui cadru legislativ eficient și armonizat cu legislația europeană în domeniu.

# Exercițiul de securitate cibernetică CyDEx18

CyDEx este singurul exercițiu de securitate cibernetică din Romania de tip hands on ( axat pe componenta practică) ce asigură un nivel avansat de realism prin desfășurarea activităților într-un poligon de securitate cibernetică.

Exercițiul are ca principal obiectiv exersarea capacităților de apărare în domeniul securității cibernetice împotriva amenințărilor la adresa infrastructurilor IT&C cu valențe critice pentru securitatea națională.

Demersul se înscrie în eforturile Serviciului Român de Informații de a crea un mecanism eficient de avertizare, alertă și reacție la incidentele cibernetice, precum și de a dezvolta cooperarea dintre sectorul public și cel privat în domeniul securității cibernetice.

Exercițiul de anul acesta va întruni participanți din 90 de entități din mediul public, privat și academic și spre deosebire de cel de anul trecut, CyDEx2018 va cuprinde mai multe scenarii, propuse atât de mediul public, cât și de cel privat.

> Organizarea primei ediții a exercițiului a reprezentat un beneficiu la nivel național, asigurând cadrul necesar tuturor entităților implicate să desfășoare activități comune, destinate soluționării unor atacuri cibernetice simulate cu un grad ridicat de realism. Activitatea a contribuit la conștientizarea nivelului de pregătire al diferiților actori în situația unui eveniment ce va afecta major spațiul cibernetic la nivel național.

CyDEx18 va permite:

Verificarea și stimularea mecanismelor de cooperare între instituțiile publice cu responsabilități în domeniul securității naționale și, în general, între instituțiile publice, mediul privat și cel academic;

Dezvoltarea unui mecanism eficient de avertizare, alertă și reacție la incidente de securitate cibernetică;

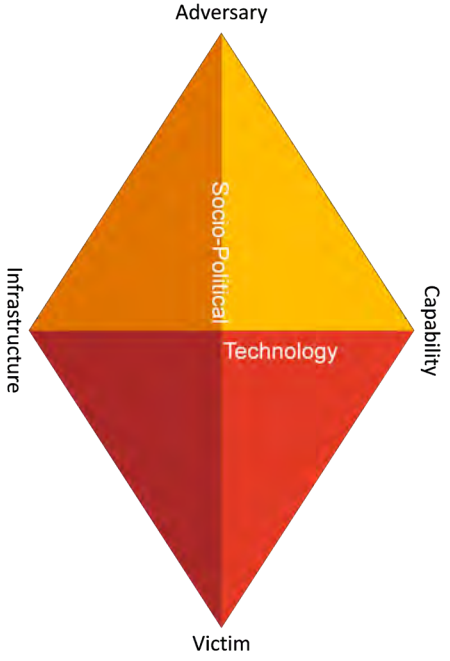
Verificarea nivelului de expertiză tehnică al specialiștilor din cadrul entităților participante în cazul unui incident cibernetic major la nivel național;

Creșterea nivelului de conștientizare, atât la nivelul instituțiilor publice, cât și la nivelul celor private cu privire la amenințările din spațiul cibernetic, precum și la efectele unui incident cibernetic major la nivel național.

# **Investigarea** atacurilor cibernetice din perspectiva activității de intelligence

Una dintre tehnicile analitice utilizate de experții SRI pentru o mai bună înțelegere și investigare a atacurilor cibernetice complexe, de regulă de tip APT, este Diamond Model. Dezvoltat de cercetători și experți din domeniul securității cibernetice, modelul oferă o metodă de prioritizare și ierarhizare inițială a datelor cunoscute, dar și un punct de plecare într-o eventuală investigație a unui atac cibernetic.

Din punct de vedere grafic, modelul este reprezentat printr-un romb ale cărui diagonale




semnifică cele două coordonate care trebuie avute în vedere atunci când se efectuează o analiză a unui atac cibernetic de tip APT: axa socio-politcă (în extremități fiind marcate victimele și atacatorul) și axa tehnologică (cu extremitățile - infrastructură și capabilități). Forma grafică ne ajută la integrarea datelor avute la începutul investigației, deoarece prin suprapunerea a două sau mai multe astfel de romburi, se pot compara activitățile unor actori neidentificați până la momentul analizei, cu unii deja cunoscuți. Asemănările și deosebirile dintre aceste modele pot conduce către concluzii care să asigure, cu un grad ridicat de probabilitate, atribuirea activității din spațiul cibernetic unui atacator deja cunoscut.

Analiza elementelor inventariate pe axa socio-politică în cazul unei amenințări la adresa securității naționale, poate oferi informații relevante pentru o organizație de intelligence, a cărei arie de competență include și domeniul securității cibernetice. Astfel, sunt de interes țintele care pot conduce o investigație către concluzii relevante referitoare la motivația unui actor cibernetic, la domeniile vizate, dar și către conexiuni cu obiectivele unui actor statal.

Ca urmare a analizei acestor informații se poate realiza o estimare a complexității și persistenței unui atac cibernetic. Mai mult, statutul de putere globală sau regională a unui stat, prezumat a fi în spatele unui atac cibernetic, poate conduce către concluzii relevante în ceea ce privește gradul de alocare de resurse financiare și umane.

Pe axa tehnologică a modelului se inventariază elemente de infrastructură de comandă și control utilizate în atacul supus analizei, dar și tactici, tehnici și proceduri (TTP) care pot reieși în urma investigației.

De interes din acest punct de vedere este nivelul de complexitate și anonimizare al infrastructurii și al instrumentelor utilizate în atac. Prin compararea acestor atacuri cibernetice cu altele deja cunoscute și analizate prin Modelul Diamond, pot fi emise concluzii relevante legate de similitudinea parțială sau totală a activității unor grupări de actori cibernetici. De asemenea, investigarea acestor aspecte este în măsură să redea o serie de detalii necesare diminuării efectelor atacului.

Modelul Diamond este doar una dintre tehnicile de analiză a informațiilor care poate fi aplicată în investigarea atacurilor cibernetice statale. Pentru a se obține rezultate eficiente în demersul investigativ, este necesară aplicarea mai multor metode, dar și coroborarea mai multor surse de informații. Cu toate acestea, modelul poate oferi un punct de plecare în ceea ce privește investigarea unui atac cibernetic, deoarece poate organiza o serie de informații în categorii relevante.

# Trend tehnologic: *Cloud Computing*

Cloud computing-ul, cunoscut și sub numele de cloud, constă în rețele de centre de date la care, atât utilizatorii individuali, cât și entitățile publice și private, își pot conecta dispozitivele, permițându-le astfel accesarea de resurse de calcul prin Internet. Cloud-ul are caracteristici specifice în comparație cu soluțiile administrate local, utilizate în mod tradițional, cum ar fi capacitatea de stocare și de calcul crescută și posibilitatea de acces de la distanță.

Astfel, cloud-ul determină reorientarea utilizatorilor de la modelul convențional de infrastructură IT&C, în care stocarea și procesarea datelor se realiza pe infrastructura proprie, către cel în care aceste activități sunt realizate folosind infrastructură externalizată.

Tehnologia Cloud Computing poate fi clasificată în funcție de următoarele servicii:

## Infrastructure-as-a-Service (IaaS)

Prin acest serviciu clienților li se permite să externalizeze furnizarea funcțiilor de calcul de bază, beneficiind de fiabilitatea, scalabilitatea și rentabilitatea pe care le oferă cloud-ul. Infrastructura utilizată nu este administrată de client, acesta având control doar asupra sistemelor de operare și a aplicațiilor rulate.

## Platform as a Service (PaaS)

Furnizorii de tehnologie cloud găzduiesc, în cadrul infrastructurii proprii, instrumentele necesare dezvoltatorilor de software care pot fi accesate prin intermediul unei interfețe de programare a aplicațiilor (API - Application Programming Interface) sau a portalurilor web.

## Software as a Service (SaaS)

Este cea mai familiară formă a tehnologiei cloud și presupune furnizarea de acces la aplicații web prin intermediul Internetului. Datorită numeroaselor avantaje pe care le implică tehnologia cloud, utilizatorii pot integra în propriile activități servicii multiple, mai avantajoase din punct de vedere al accesibilității și eficienței, precum:

## Aplicații de comunicații

Acestea funcționează pe o infrastructură cloud, mesajele fiind stocate pe servere puse la dispoziție de furnizori și nu pe propriul telefon al utilizatorului, permițând accesul la informații de oriunde, prin Internet. Cele mai utilizate aplicații de acest tip sunt WhatsApp, Skype, Telegram, Facebook Messenger.

## Analiză big data

Utilizarea cloud computing în dezvoltarea unor instrumente de analiză big data[3] permite analiștilor să realizeze corelații, să identifice tipare și să acumuleze cunoaștere, pe baza unei cantități mari de date, oferind, astfel, suport în adoptarea unor decizii. Hadoop, Cassandra, HPCC sunt câteva exemple de produse software ce pot fi utilizate în acest scop.

## Rețele de socializare

Dezvoltarea rețelelor de socializare prin utilizarea tehnologiei cloud permite o interacțiune mai bună a utilizatorului acestui tip de platformă. Astfel, o serie de funcționalități ale rețelelor de socializare, precum căutarea în funcție de o serie de criterii complexe sau diversificarea conținutului ce poate fi vizualizat, au cunoscut o creștere calitativă în ultimii ani. În context, pe fondul fluxului continuu de date, utilizarea serviciilor cloud este esențială pentru a asigura funcționarea optimă a infrastructurii IT&C necesară.

Pentru a asigura securitatea unui cloud este necesară implementarea de politici și proceduri de securitate, iar furnizorii trebuie să dea dovadă de transparență, comunicându-le clienților aspectele relevante cu privire la componenta de securitate cibernetică a serviciilor pe care le oferă. Spre exemplu, marii furnizori de tehnologie cloud utilizează sisteme complexe de criptare și politici de securitate menite să reducă nivelul de vulnerabilizare a infrastructurii respective și, implicit, incidența atacurilor cibernetice derulate prin exploatarea acestora.

*[3] Colecție de seturi de date, structurate și nestructurate, ale căror dimensiuni sunt prea mari și complexe pentru a putea fi gestionate de aplicațiile de procesare analitică tradiționale.*


www.sri.ro