**Securitate cibernetică și tehnologiile blockchain**

de Mehmet Ali ERTURK

*Universitatea din Istanbul (Turcia)*

Bună ziua și bine ați venit. Astăzi vom analiza pe scurt două tehnologii care sunt esențiale în procesele de digitalizare: securitatea cibernetică și blockchain.

Trăim într-o lume digitală – calculatoarele, tehnologiile informației și dispozitivele electronice sunt implicate în fiecare aspect al vieții noastre. De exemplu, ne folosim computerele personale atunci când predăm cursuri online sau ceasurile inteligente atunci când ne înregistrăm și ne monitorizăm datele de sănătate. Folosim bancomatele pentru a transfera bani sau ne folosim calculatoarele pentru site-uri de comerț electronic cu cardurile noastre de credit. În plus, ne păstrăm toate informațiile personale sau instituționale în aplicații de tip cloud. Toate aceste procese au loc pe ceea ce numim sisteme informatice.

Așadar, ce este un computer sau ce este un dispozitiv de calcul? Calculatoarele sunt dispozitive electronice concepute pentru a executa automat operații logice și aritmetice. Intrarea, procesarea, ieșirea și stocarea sunt funcțiile principale ale calculatoarelor. De exemplu, dacă dorim să adunăm două numere, cele două numere reprezintă intrarea, adunarea celor două numere reprezintă procesul, iar rezultatul este afișat ca ieșire. Dacă dorim să păstrăm rezultatul, folosim funcțiile de stocare.

Sistemele informatice pot fi la fel de mici precum un smartwatch sau foarte mari precum supercomputerele. În principal, computerele noastre au două componente principale: una este hardware-ul, iar cealaltă este software-ul. Hardware-ul este componenta fizică care alcătuiește întregul computer; este vorba de părțile pe care le putem atinge. Software-ul este colecția de programe care rulează pe sistemele informatice. Programele conțin instrucțiuni care spun calculatoarelor ce să facă. De exemplu, am putea avea software util, cum ar fi browserele noastre pe care le folosim toată ziua pentru a naviga pe internet. Cu toate acestea, este posibil ca unele software-uri sau unele programe să nu fie la fel de bune în browserele noastre. Un software rău intenționat, de exemplu, poate încerca să ne facă rău nouă sau sistemelor noastre informatice.

Așa cum am menționat deja, calculatoarele sunt dispozitive programabile care lucrează pe baza datelor. Putem defini datele ca fiind un element, de pildă litere, numere, imagini ori videoclipuri, pe care sistemele informatice îl pot utiliza. Informația este o formă de date care este prelucrată pentru a deveni semnificativă. De fapt, nu avem nevoie de computere pentru a prelucra informații; cu toate acestea, dispozitivele informatice ne ușurează viața și ne permit să obținem rezultate exacte cu mai puțin efort. De asemenea, ne folosim computerele și dispozitivele mobile pentru a trimite date pe internet și pentru a împărtăși informațiile noastre cu alții.

În ceea ce privește internetul, acesta este infrastructura de comunicare în lumea digitală de astăzi. Este o rețea de rețele. Istoria internetului datează de la începutul anilor 1960. Acesta a fost utilizat inițial în scopuri militare și științifice. De-a lungul timpului, odată cu creșterea interesului public și a utilizării pe scară largă, internetul a devenit parte din viața noastră. În prezent, în multe țări este posibil să se acceseze rețele 5G, i.e. de a cincea generație. Datorită legăturilor de comunicare de mare viteză și latență redusă, ceea ce era un vis în trecut este posibil astăzi. De exemplu, atunci când se utilizează 5G, medici din diferite părți ale lumii pot participa și colabora la o operație de chirurgie robotică. De asemenea, odată cu extinderea infrastructurii 5G, multe obiecte pot avea acum cu ușurință o conexiune la internet, iar aceste obiecte pot fi gestionate de la distanță.

Aceste conexiuni omniprezente ridică o întrebare: cum putem ca viața noastră să rămână privată în această lume digitală? Digitalizarea a redus semnificativ efortul pentru a avea acces la informații, însă în același timp și comiterea de infracțiuni în domeniul digital a devenit mult mai ușoară. Hackeri cu diferite motivații pot pătrunde în computere, deturna conturi cu legătură la internet, scurge date din companii, modifica date ale unor instituții sau chiar opri rețelele electrice.

Securitatea cibernetică, sau securitatea informațiilor, este studiul protejării sistemelor, rețelelor și datelor împotriva atacurilor neautorizate. Scopul securității cibernetice este de a păstra coerența datelor noastre și de a preveni accesul neautorizat.

În prezent, există diferite tipuri de amenințări cibernetice disponibile. În această prezentare, vom discuta pe scurt cele mai cunoscute metode.

Malware-ul este un software malițios conceput pentru a obține acces la sistemele informatice. Dispozitivele afectate de acest software pot efectua operațiuni împotriva intenției utilizatorului. Acesta poate provoca daune sau fura informații. De asemenea, computerul gazdă poate deveni un vector pentru hackeri și infractori, astfel încât infractorii își pot ascunde identitatea și comite infracțiuni folosind aceste computere. Există o mulțime de tipuri de malware disponibile în prezent, însă cel mai popular este ransomware-ul. Ransomware criptează sistemul de fișiere al victimei în schimbul unei răscumpărări și blochează accesul. Acesta rezultă, de obicei, din apăsarea unui link rău intenționat într-un e-mail sau într-o aplicație de mesagerie instantanee, iar uneori nu este ușor să recuperați datele criptate.

Phishing-ul este un alt tip de atac în care victimelor li se trimit e-mailuri cu link-uri false. Motivația hackerilor este să fure bani sau date sensibile de la victime. Aceștia trimit linkuri false prin e-mailuri sau prin alte platforme pentru a redirecționa victimele către o pagină web unde le pot fura cu ușurință datele de identificare.

Atacurile de tip Denial of Service (DoS) sunt un tip de atac diferit de malware. În atacurile DoS este vizată o rețea sau un serviciu de internet pentru a-l face inaccesibil temporar sau permanent pentru utilizatorii vizați. De exemplu, un atac DoS îndreptat împotriva unei infrastructuri electronice, cum ar fi e-guvernarea, poate bloca accesul cetățenilor la serviciile acesteia. Există mai multe tipuri de atacuri DoS care utilizează diverse tehnici, cum ar fi atacurile de tip DDoS (distributed denial of service).

Un alt tip de atac este atacul APT – amenințare persistentă de nivel avansat (eng. Advanced Persistent Threat). De obicei, aceste tipuri de atacuri necesită cunoștințe și resurse avansate pentru a fi efectuate. Aceste tipuri de atacuri sunt de obicei finanțate de organizații sau guverne. Atacurile APT sunt destul de sofisticate și urmăresc să obțină acces la un sistem, pentru o perioadă lungă de timp și nedetectat, permițând infractorilor să inspecteze aceste sisteme în profunzime.

Așadar, ce face ca sistemele informatice să fie nesigure în fața acestor amenințări? Există câteva metode sau câțiva factori care fac aceste sisteme nesigure. Voi menționa doar trei dintre aceștia.

Primul este legat de proiectare – hardware sau software. Inginerii ar trebui să ia în considerare caracteristicile de securitate atunci când proiectează un sistem. Proiectele care nu țin cont de securitate au ca rezultat sisteme defectuoase care sunt deschise la exploatări care vor permite atacatorilor să obțină acces.

Al doilea motiv este configurarea greșită. Un sistem poate fi proiectat ținând cont de securitate; cu toate acestea, erorile în configurarea securității pot duce la potențiale scurgeri de informații. Un sistem conceput pentru a fi foarte sigur trebuie să fie actualizat pentru a permite revenirea la configurația inițială și pentru a face față noilor amenințări.

Al treilea motiv sunt oamenii. Atâta timp cât oamenii sunt implicați, există întotdeauna un risc de securitate. De exemplu, orice acțiune greșită a unui angajat poate face ca un sistem intern să fie infectat cu viruși sau troieni. De asemenea, un angajat nemotivat ar putea fura datele companiei sale sau ar putea permite infractorilor să acceseze aceste sisteme. Niciun sistem nu poate fi 100% sigur; cu toate acestea, avem instrumente cu ajutorul cărora putem lua măsuri.

Primul și cel mai important lucru este conștientizarea securității cibernetice. Acesta este procesul de educație care prezintă amenințările cibernetice și modul de a lua măsurile de precauție necesare. Aceste cursuri de formare ar trebui oferite în mod regulat utilizatorilor de la diferite niveluri și ar trebui repetate periodic pentru a crește gradul de conștientizare a amenințărilor la adresa securității.

În plus, avem soluții de securitate hardware și software care împiedică accesul neautorizat la sistemele noastre. De exemplu, avem firewall-uri care monitorizează traficul de rețea și analizează datele de intrare și de ieșire pentru a aplica reguli de securitate predefinite. Acestea pot bloca sau permite cererile de acces de la servere la utilizatori. Firewall-urile pot funcționa la orice nivel – fizic, rețea sau aplicație. Există versiuni specifice ale firewall-urilor dedicate aplicațiilor web, denumite firewall-uri pentru aplicații web (WAF), care conțin reguli de securitate specifice aplicațiilor web.

Un alt instrument este sistemul de detectare a intruziunilor (IDS). Acesta utilizează metode analitice avansate pentru a genera alerte cu privire la activitatea suspectă din rețea sau din cadrul unei companii. Pentru a da un exemplu concret, ne putem configura firewall-urile astfel încât doar setul de servicii pe care le permitem să fie accesibile din afara organizației, astfel încât persoanele neautorizate să nu se poată conecta la serverele din spatele firewall-urilor. Un alt exemplu este că ne putem folosi WAF-urile pentru a bloca atacurile care doresc să infesteze serverele noastre web prin exploatarea vulnerabilităților ce permit conectarea la procesele de interogare a bazelor de date (SQL injection). Orice cerere cu activitate suspectă va fi blocată de firewall-urile noastre pentru aplicații web. De asemenea, putem utiliza sistemele IDS pentru a identifica și a genera alerte atunci când angajații acționează în afara tiparelor lor obișnuite. De exemplu, dacă un angajat încearcă să acceseze fișiere de la locul de muncă dintr-o locație neobișnuită, sistemul IDS poate genera un avertisment, iar această situație poate fi raportată managerului de securitate.

Putem discuta multe alte exemple, dar să trecem la un alt mecanism de prevenție, autentificarea. Autentificarea este un mecanism care verifică dacă utilizatorii sunt ceea ce pretind a fi. Au fost dezvoltate diverse metode de autentificare, dar esențială este cea care necesită nume de utilizator și o parolă pentru că această metodă este folosită zilnic în serviciile online.

În prezent, malware-ul, virușii, ransomware-ul și troienii (malware deghizat ca program obișnuit) se răspândesc rapid. Programele antivirus sunt instrumente de securitate dezvoltate pentru a preveni impactul acestor programe dăunătoare asupra calculatoarelor și serverelor noastre.

O altă metodă pe care o putem folosi pentru a rămâne în siguranță în lumea online este criptarea. Aceasta este o metodă prin care informațiile sunt modificate în așa fel încât observatorii să nu le poată citi în timp ce sunt transmise pe internet. Numim textul necitit cifru. Sunt disponibili algoritmi matematici avansați pentru a crea o criptare puternică, astfel încât aceasta să nu poată fi decodată prin intervenție externă. În prezent, dispunem de algoritmi criptografici simetrici și asimetrici pentru a ne securiza, restaura datele sau transmite pe un canal de comunicare.

Putem dezvolta sisteme sigure, persistente și modificabile împotriva atacurilor cibernetice prin criptare și algoritmi criptografici. Unul dintre cazurile de utilizare sunt tehnologiile blockchain. Blockchain este un registru digital descentralizat, i.e care este distribuit în rețea. Fiecare set de date este un bloc (eng. block) și seturile sunt legate cronologic unele de altele ca într-un lanț (eng. chain). Ideea a fost introdusă pentru prima dată în 1991; cu toate acestea, tehnologia a devenit populară odată cu criptomoneda digitală Bitcoin. Atunci când rețeaua descentralizată Bitcoin, bazată pe încredere, a introdus-o, aceasta a captat atenția lumii, iar ideea de registru digital a început să apară în diverse aplicații.

Un sistem distribuit nu are nevoie de gestionare centrală, iar rețeaua ia măsurile necesare. De exemplu, sistemul bancar actual este centralizat și necesită o autoritate care să îi reglementeze toate operațiunile. Banca se ocupă de toți pașii necesari dacă cineva trebuie să trimită bani către o altă entitate. În schimb, sistemele distribuite precum blockchain și criptomonedele bazate pe blockchain funcționează direct de la un utilizator la altul (eng. peer-to-peer). O persoană poate trimite bani direct unei alte entități fără a avea nevoie de o bancă.

Atât sistemele centralizate, cât și cele distribuite au avantajele și dezavantajele lor. Principalul dezavantaj al unui sistem distribuit este timpul de execuție. Arhitecturile centralizate permit tranzacții mai rapide deoarece totul este centralizat. Operațiunile din sistemele distribuite pot necesita multă muncă și mult timp; cu toate acestea, oferă libertate de alegere.

Blockchain se bazează pe algoritmi criptografici securizați și pe metode de consens care permit ca informațiile să fie persistente, valide și nemodificabile în întreaga rețea. Pur și simplu, o înregistrare este o reprezentare a unei singure tranzacții (un bloc), iar aceste blocuri sunt legate între ele pentru a construi blockchain-ul. Blockchain este pur și simplu un sistem de baze de date distribuite care nu necesită o autoritate centrală. Fiecare nod din rețea poate funcționa fără intervenție centrală. Ori de câte ori este inițiată o tranzacție, această operațiune este distribuită tuturor nodurilor din rețea și este necesar să se valideze dacă tranzacția este corectă. Dacă operațiunea este corectă, aceasta este aprobată pentru a fi persistentă în registru.

Rețelele Blockchain funcționează într-o manieră distribuită, iar operațiunile între egali ale rețelei trebuie să fie validate. Termenul tehnic pentru această validare este mecanism de consens. Mecanismul de consens este necesar pentru a verifica dacă acțiunea curentă este valabilă sau nu. Există mai mulți algoritmi pentru a asigura consensul, dar proof of work (PoW) este cel mai popular datorită criptomonedelor, cum ar fi Bitcoin. Ori de câte ori o entitate trimite Bitcoins unei alte entități, nodurile din rețea efectuează algoritmi criptografici complecși pentru a verifica dacă tranzacția este validă. Această metodă de consens distribuit se numește proof of work; cu toate acestea, PoW necesită mai multă putere de calcul și timp de execuție. Există metode alternative, cum ar fi proof of stake (PoS) și proof of identity (PoID).

Algoritmii de consens permit tuturor nodurilor din rețea să aibă aceeași stare, asigurând consistența procesului. Acest lucru înseamnă că, ori de câte ori apare o cerere de tranzacție în rețea, aceasta este validată și distribuită tuturor nodurilor, astfel încât nodurile din rețea au toate aceleași informații.

De asemenea, în rețelele blockchain, avem așa numite contracte inteligente (eng. smart contracts), i.e. programe care îndeplinesc sarcini automate pe baza unor condiții predefinite. Contractele inteligente execută acțiunile necesare pe baza termenilor și condițiilor convenite între părțile implicate. Termenii și condițiile sunt implementate ca aplicații software și executate pe noduri; dacă se întâmplă ceva, se întreprinde o anumită acțiune.

Putem utiliza contracte inteligente pentru a crea aplicații blockchain. Aplicațiile și rețelele Blockchain pot fi distribuite ca fiind publice sau private. În rețelele private, există o procedură pentru a adera la rețea numită autorizare.

Există multe aplicații pentru blockchain, care nu se limitează doar la finanțe. Această tehnologie poate fi utilizată în domeniul sănătății, de pildă pentru stocarea dosarelor individuale privind sănătatea pacienților. De asemenea, poate fi utilizat în educație, logistică și Internetul obiectelor (IoT). Un alt domeniu de aplicabilitate este e-guvernarea. De exemplu, un sistem de vot electronic poate fi implementat într-o infrastructură blockchain, astfel încât atacatorii sau infractorii să nu poată accesa sau modifica datele din rețea.

În această prelegere, am discutat două subiecte importante, și anume securitatea cibernetică și blockchain.

Vă mulțumesc.

--

*Acest material a fost înregistrat în limba engleză la Universitatea din Tartu (Estonia) în martie 2023. Traducerea a fost realizată după transcrierea în limba engleză și a fost editată din motive de claritate.*

**Cum poate fi citat acest text**

Mehmet Ali ERTURK (2023) *Securitatea cibernetică și tehnologiile blockchain*.Material elaborat în cadrul proiectului Erasmus+ 2021-1-TR01-KA220-HED-000027609 “Digital Diplomacy: Building the Common Future with Technology (DD-Tech)”. Tartu: Universitatea din Tartu.