A-Z

GLOSAR
DE TERMENI PENTRU DOMENIUL
SECURITĂȚII CIBERNETICE

PREZENTAREA GLOSARULUI

CE ESTE

Materialul este un glosar alcătuit din termeni specifici sau aflați în legătură cu domeniul de studiu al securității cibernetice. Conține atât termeni de bază, cât și denumirile unor amenințări sau vulnerabilități specifice.

CUM A FOST REALIZAT

Definițiile termenilor au fost preluate din surse cu grad ridicat de credibilitate, documente oficiale și alte dicționare de specialitate, ulterior fiind integrate și prelucrate pentru a obține o compilație a celor mai relevanți și utilizați termeni în domeniul securității cibernetice.

CE ÎȘI PROPUNE

Să explice, într-o manieră simplă, atât termeni de bază, cât și complecși din domeniul cibernetic, celor ce doresc o inițiere în acest domeniu, chiar dacă nu dețin o pregătire avansată în domeniul tehnic. Domeniul securității cibernetice conține o multitudine de termeni specifici care nu sunt utilizați în conversațiile cotidiene, motiv pentru care glosarul oferă acces ușor și rapid la definiții simple și scurte ale celor mai utilizați termeni din domeniul securității cibernetice.

ABREVIERILE TERMENILOR

Mențiune: În conținutul dicționarului termenii vor fi regăsiți cu denumirea lor integrală. Înainte de a căuta un termen abreviat, consultați lista de abrevieri.

0 day - Zero day exploit/vulnerability
2FA - Two factor authentication
ACL - Access Control List
AES - Advanced Encryption Standard
AI - Artificial Intelligence
API - Application Programming Interface
APT - Advanced Persistent Threat
ATD - Advanced Threat Defense
AV - Antivirus
BCP - Business Continuity Plan
BGP - Border Gateway Protocol
BIOS - Basic Input Output System
BPH - Bullet Proof Hosting
BYOD - Bring Your Own Device
CAV - Counter Antivirus
CDN - Content Distribution Network
CEH - Certified Ethical Hacker
CIA - Confidentiality, Integrity and Availability
CLI - Comand Line Interface
CMS - Content Management System
CNO - Computer Network Operations
CPU - Central Processing Unit
CSIRT - Computer Security Incident Response Team
CSMA/CD - Carrier-sense multiple access with collision detection
CSRF - Cross Site Request Forgery
CVE - Common Vulnerabilities and Exposures
DoS - Denial of Service
DDoS - Distributed Denial of Service
DLP/ILP - Data/Information Loss Prevention
DLT - Distributed Ledger Technology
DMZ - Demilitarized zone

DNS - Domain Name System
DRM - Digital Rights Management
E2EE - End-to-end encryption
FDE - Full Disk Encryption
FPD - Full Path Disclosure
FTP - File Transfer Protocol
FVF - Finding Vulnerabilities and Flaws
GUI - Graphical User Interface
HOIC - High Orbit Ion Cannon
HTML - Hyper Text Markup Language
HTTP - Hyper Text Transfer Protocol
HTTPS - Hyper Text Transfer Protocol/Secure
IDS - Intrusion Detection System
IM - Instant messaging
IMAP - Internet Message Access Protocol
IMSI - International Mobile Subscriber Identity
InfoSec - Information Security
IoC - Indicators of Compromise
IoT - Internet of Things
IP - Internet Protocol
IPS - Intrusion Prevention System
IR - Incident Response
IRC - Internet Relay Chat
IRCd - Internet Relay Chat daemon
ISP - Internet Service Provider
IT&C - Information Technology and Communications
LAN - Local Area Network
LFI - Local File Inclusion
LOIC - Low Orbit Ion Cannon
MAC - Media Access Control
MBR - Master Boot Record
NAS - Network Attached Storage
NAT - Network Adress Translation
NFC - Near Field Communication
NLA - Network Level Authentification
OSINT - Open Source Intelligence
P2P - Peer-to-peer

PaaS - Platform as a Service
PAN - Personal Area Network
PHP - Php: Hypertexted Preprocessor
PLC - Programmable Logic Controllers
PoC - Proof of Concept
PUP - Potentially Unwanted Program
RAM - Random Access Memory
RAT - Remote Access Tool/Trojan
RCE - Remote Code Execution
RDC - Remote Desktop Connection
RDP - Remote Desktop Protocol
RFI - Remote File lnclusion
ROM - Read Only Memory
RSA - Rivest-Shamir-Adleman
RTO - Recovery time objective
RTU - Remote Terminal Unit
SCADA - Supervisory Control and Data Acquisition System
SEO - Search Engine Optimization
SFTP - Secure File Transfer Protocol
SHA - Secure Hash Algorithm
SHTTP - Secure Hyper Text Transfer Protocol
SIEM - Security Information and Event Management
SMB - Server Message Block
SPA/SPOA - Single Point of Accountability
SQL - Structured Query Language
SQLi - SQL Injection
SSH - Secure shell
SSID - Service Set Identifier
SSL - Secure Sockets Layer
TCP - Transmission Control Protocol
TFTP - Trivial File Transport Protocol
TLS - Transport Layer Security
TOR - The Onion Router
TTP - Tactics, Techniques and Procedures
VEP - Vulnerabilities Equities Process
VM - Virtual Machine
VoIP - Voice over Internet Protocol

VPN - Virtual Private Network
VPS - Virtual Private Server
UCP - Unitate Centrală de Procesare
UDP - User Datagram Protocol
UI - User Interface
URI - Uniform Resource Identifier
URL - Uniform Resource Locator
URN - Uniform Resource Name
USB - Universal Serial Bus
UTM - Unified Threat Management
WAN - Wide Area Network
WEP - Wired Equivalent Privacy
WLAN - Wireless Local Area Network
WPA - Wi-Fi Protected Access
WWW - World Wide Web
XSS - Cross-site scripting

A de la APT

Acces Proces bazat pe un set de reguli și drepturi conferite unui utilizator pentru a vizualiza și utiliza anumite funcții din sisteme, rețea, aplicații sau componente hardware.

Access Control List (ACL) Listă prin intermediul căreia sunt stabilite rolurile și acțiunile pe care le pot efectua utilizatorii în cadrul unui sistem IT&C.

Acces de la distanță Accesul unui utilizator la o resursă IT&C prin intermediul unei alte resurse IT&C aflată în afara rețelei locale din care face parte sistemul accesat. *Exemplu: prin intermediul Internetului.*

Acces neautorizat (Unauthorized acces) Accesarea unui sistem IT&C sau a unei rețele fără a deține permisiuni.

Acreditare Declarație formală din partea unei autorități, prin care un sistem informațional beneficiază de avizul de funcționare, pe baza implementării unui set aprobat de măsuri de protecție tehnică, managerială și procedurală.

Actor cibernetic Persoană, grup de persoane sau organizație care realizează atacuri cibernetice.

Add-on (Plug-in) Aplicație de mici dimensiuni care modifică sau adaugă noi funcționalități web browser-ului. *Vezi și* Browser.

Administrator (de sistem/rețea) Persoană responsabilă de configurarea, mentenanța și managementul funcțiilor și rolurilor în cadrul unui sistem sau rețea IT&C. *Vezi și* Mentenanță.

Advanced Encryption Standard (AES) Cunoscut și sub numele de Rijndael, reprezintă un algoritm standardizat pentru criptarea simetrică (este utilizată aceeași cheie atât pentru criptare, cât și pentru decriptare). *Vezi și* Data Encryption Standard și Criptare simetrică.

Advanced Persistent Threat (APT) Concept utilizat pentru a defini un atac cibernetic derulat, de regulă, de o entitate statală, ce vizează ținte strategice (din domeniul guvernamental, militar, al securității naționale și/sau al afacerilor), care prin intermediul tehnicilor, tacticilor și procedurilor de nivel ridicat, reușește să fie nedetectabil o perioadă lungă de timp cu scopul de a extrage date pentru a obține avantaje strategice sau financiare.

Advanced Threat Defense (ATD) Concept utilizat de companiile de securitate cibernetică pentru a defini un produs cu posibilități tehnice ridicate de detecție, prevenire și combatere a tentativelor neautorizate de intruziune în rețeaua protejată.

Adresă IP Cod de identificare al dispozitivelor, la nivel de rețea, care facilitează comunicarea între dispozitive aflate în rețele diferite (inclusiv Internet) sau în cadrul aceleiași rețele. *Vezi și* Internet Protocol.

Adware (advertising-supported software) Aplicație nelegitimă care colectează date și informații despre activitatea utilizatorului, pe baza cărora promovează reclame la produse și/sau servicii. Ulterior instalării, în anumite situații, descarcă și alte aplicații nelegitime fără consimțământul utilizatorului.

Air gap Folosirea unei forme de separare fizică a unor dispozitive IT&C cu scopul de a asigura securitatea activităților și fișierelor de pe toate dispozitivele implicate. În cazul în care un dispozitiv este infectat, scopul este de a-l izola astfel încât să nu interacționeze cu alte sisteme sau rețele ce nu au fost compromise. *Vezi și* Air gap malware.

Air gap malware Software nelegitim conceput să infecteze dispozitivele protejate prin metoda air gap. Una dintre cele mai cunoscute metode prin care se realizează propagarea unui astfel de malware este prin utilizarea unui suport de memorie externă pentru transferul datelor între rețele. *Vezi și* Air gap și Malware.

Alertă Notificare cu privire la un potențial atac cibernetic îndreptat împotriva sistemelor sau rețelelor IT&C ale unei organizații.

Algoritm Set de instrucțiuni structurate logic destinat rezolvării unei probleme, realizării unei proceduri de calcul, procesării unor date sau studierii unor procese.

Amenințare cibernetică Circumstanță sau eveniment care constituie un pericol potențial la adresa securității cibernetice. *Vezi și* Confidentiality, Integrity and Availability.

Analiză de trafic Obținerea de informații prin studiul caracteristicilor observabile din fluxul pachetelor de date generate de un dispozitiv. Este utilizată pentru a extragerea conținutului informațional cuprins în comunicațiile efectuate de acel dispozitiv. Wireshark este cel mai cunoscut exemplu de aplicație gratuită prin care se analizează fluxul pachetelor de date și este utilizată inclusiv pentru soluționarea problemelor în rețea si dezvoltarea produselor software și a protocoalelor de comunicare.

Analiză malware Procesul de determinare a funcționalităților, a originii și a impactului aplicațiilor malware. *Vezi și* Malware.

Anti-malware Software conceput să blocheze accesul sau să caute, izoleze și să elimine fișierele și aplicațiile cu conținut malware. *Vezi și* Malware.

Anti-spyware Software conceput să blocheze accesul sau să caute, izoleze și să elimine fișierele și aplicațiile care monitorizează activitatea și extrag informații confidențiale. *Vezi și* Spyware.

Antivirus (AV) Software conceput să blocheze accesul sau să caute, izoleze și să elimine o gamă foarte largă de fișiere și aplicații nelegitime.

Aplicație (Software) Program care execută una sau mai multe funcții în mod direct pentru un utilizator prin crearea, modificarea, procesarea, stocarea, inspectarea sau transmiterea unor tipuri specifice de date, fără a necesita în mod obligatoriu privilegii de control, monitorizare sau administrare.

Application Programming Interface (API) Set de proceduri și reguli care facilitează dezvoltarea aplicațiilor care accesează date și funcții ale altor aplicații, servicii sau sisteme de operare.

Arhitectură de rețea Modul de structurare al echipamentelor hardware și software din cadrul unei rețele. *Vezi și* Rețea.

Arhitectură de securitate cibernetică Model ce integrează soluții de securitate cibernetică cu scopul prevenirii și detecției atacurilor cibernetice.

Artificial Intelligence (AI) *Vezi* Inteligența artificială.

Atac cibernetic Actiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică. *Vezi și* Confidentiality, Integrity and Availability.

Atac de rețea Atac care vizează perturbarea rețelelor și utilizatorilor acesteia prin manipularea protocoalelor de comunicare. Cele mai folosite metode de atac: spoofing, session hijacking, atacuri wireless și atacuri prin aplicații web.

Atacuri la parole Atac care vizează identificarea parolei și accesul la informația restricționată prin intermediul acesteia. Cele mai folosite metode de atac: dictionary attack, rainbow tables și brute force.

Atribuire Procesul de analiză a dovezilor și indiciilor unui atac cibernetic, care are ca scop identificarea entității care l-a derulat.

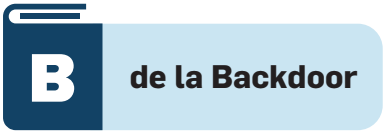
Audit de sistem Evaluarea, examinarea și controlul independent al datelor și activităților, în vederea stabilirii parametrilor funcționali ai sistemului și asigurării conformității cu politicile și procedurile operaționale. Toate aceste date sunt incluse într-un log de audit, care reprezintă o înregistrare cronologică a activităților din sistem. Include înregistrări ale accesărilor din sistem și operațiilor realizate într-o perioadă determinată.

Autenticitate Procesul prin care este confirmat faptul că elementele și proprietățile unei entități sunt valide.

Autentificare Procesul de verificare a identității sau a altor atribute presupuse a aparține unei entități (utilizator, proces, dispozitiv). Acest proces are următoarele elemente:
- *Mecanism de autentificare* - metodă utilizată pentru stabilirea identității utilizatorilor, dispozitivelor sau a proceselor anterior accesului.
- *Perioadă de autentificare* - perioada maximă de timp acceptată, între orice proces de autentificare și cel de reautentificare, pe durata unei sesiuni unice.
- *Protocol de autentificare* - modalitatea prin care se realizează schimbul de date între solicitant și procesul care confirmă identitatea solicitantului.

Autentificare în doi sau mai mulți factori (2FA) Utilizarea într-o manieră succesivă și conjugată a mai multor elemente pentru a dovedi identitatea persoanei sau dispozitivului care solicită acces. *Exemple: parola, token, card, date biometrice, cod transmis prin SMS etc.*

Autorizare Acțiunea de a acorda privilegii de acces unui utilizator, program sau proces.



Backdoor Facilități de tip hardware sau software care permit atacatorului să acceseze de la distanță diverse sisteme IT&C prin ocolirea sistemelor de securitate, fără ca utilizatorul să realizeze acest aspect.

Backup Procedură aplicată periodic prin care se salvează datele din cadrul unui sistem IT&C, pentru a facilita restaurarea acestora, în eventualitatea unor evenimente disruptive. *Exemple: pierderi de date, erori de sistem, erori umane etc.*

Bandwidth (Lățime de bandă) Volumul de date care poate trece printr-o rețea într-o anumită perioadă de timp.

Banner Element cu conținut grafic sau text afișat pe o pagină web cu scop de promovare și/sau redirectare către alt site/site-uri.

Banner grabbing Procesul de colectare și analiză a informațiilor de identificare a anumitor tehnologii sau sisteme utilizate la nivelul unui dispozitiv sau a unei infrastructuri.

Basic Input Output System (BIOS) Este primul software pe care îl rulează computerul când este pornit și face legătura dintre hardware (componentele fizice) și software (sistemul de operare).

Big data Colecție de seturi de date, structurate și nestructurate, ale căror dimensiuni sunt prea mari și complexe pentru a putea fi gestionate de sistemele de tip bază de date și aplicațiile tradiționale de procesare analitică.

Bit (Binary Digit) Cea mai mică unitate de măsură a cantității de informație, reprezentată în sistem binar, care poate avea valoarea 0 sau 1.

Bitcoin Lansată pe piață în 2009, este prima și cea mai populară criptomonedă din lume.

Black-box pen-testing Test de penetrare a unui sistem despre care nu se dețin date sau informații de natură tehnică. *Vezi și* Pen-testing.

Blacklisting Procedură prin care se raportează și se listează pe site-uri dedicate (blacklists) anumite adrese web sau clase de adrese IP aparținând unor sisteme sau rețele care au fost implicate în incidente de securitate cibernetică (atacuri, spam, etc.) pentru a preveni accesarea acestora și materializarea unor amenințări cibernetice.

Blame and shame Listarea unor activități ale unui actor din spațiul cibernetic și publicarea unor argumente de susținere, de către o entitate statală, în vederea descurajării întreprinderii unor acțiuni similare. *Vezi și* Atribuire.

Blockchain (tehnologia blocurilor) Registru de date organizat în blocuri de informație înlănțuite, partajate, replicate și sincronizate între membrii rețelelor de tip DLT. Principiile care stau la baza blockchain sunt criptografia și absența unui intermediar (rețelele de tip peer-to-peer). Este utilizat și în realizarea tranzacțiilor de criptomonedă. *Vezi și* Distributed Ledger Technology și Peer-to-peer.

Blue Team Echipă formată din persoane care au rolul de apărare a sistemelor informatice împotriva echipei de atacatori (Red Team), în cadrul unui concurs de hacking, în conformitate cu un set de reguli stabilite și cu monitorizare din partea unui grup neutru, cu rol de arbitru (White Team). *Vezi și* Red Team și White Team.

Bluetooth Standard utilizat pentru transmiterea de date între dispozitive, pe baza undelor radio.

Bombă cu ceas Program care generează o activitate neautorizată la un moment predefinit.

Bombă logică Element de cod introdus intenționat într-un software, care declanșează o funcție nelegitimă atunci când sunt îndeplinite anumite condiții.

Border Gateway Protocol (BGP) Protocolul de rutare care stă la baza Internetului și funcționează prin menținerea unei tabele de rețele IP care stabilește modul de conectare între sistemele autonome.

Bot Resursă IT&C care are rolul de a îndeplini sarcini simple și repetitive într-o manieră rapidă. În contextul securității cibernetice, reprezintă o dispozitiv IT&C compromis, care face parte dintr-o infrastructură alcătuită din mai multe dispozitive IT&C compromise (botnet), și care primește comenzi de la un server de comandă și control (C&C) în scopul execuției unor acțiuni nelegitime.

Botmaster (Bot herder) Hacker care, prin intermediul unui server de comandă și control (C&C), controlează o serie de echipamente IT&C compromise, care fac parte dintr-un botnet. *Vezi și* Botnet și Server C&C.

Botnet (Zombie army) Rețea de echipamente IT&C infectate, în mod intenționat, de un hacker (botmaster) și utilizate pentru derularea de atacuri cibernetice (DDoS, minare de criptomonedă, spamming etc.). Componenta software a unui botnet este formată din 2 părți: clientul și serverul de comandă și control (C&C). Botmaster-ul poate, în funcție de tipul botnet-ului, să administreze, monitorizeze și să obțină statistici cu privire la activitatea boților, prin intermediul unui panou de comandă și control. *Vezi și* Botmaster și Server C&C.

Bring Your Own Device (BYOD) Utilizarea oricărui dispozitiv electronic personal, oriunde (de obicei la muncă sau la cursuri) și oricând o impune situația.

Browser (File/Web browser) Software utilizat pentru a căuta, accesa și vizualiza un fișier stocat în cadrul unui sistem IT&C (file browser) sau a unui website (web browser). *Exemple: Internet Explorer, Mozilla Firefox, Google Chrome și Opera.*

Browsing (Navigare pe Internet) Accesarea de site-uri din Internet prin intermediul unui software specializat denumit browser. *Vezi și* Browser.

Brute force attack Metodă de acces neautorizat la un sistem IT&C sau de decodare a conținutului criptat folosind „forța brută" de calcul, prin programe care aplică metoda încercare-eroare *(trial and error)*. Metoda constă în încercarea succesivă a tuturor combinațiilor posibile de caractere, fără un algoritm elaborat. Este aplicabilă într-un număr limitat de situații, când sistemele nu sunt protejate cu parole sigure (de ex. sunt formate din prea puține caractere) sau nu au implementate mecanisme anti-brute force (sistemul *captcha* sau temporizarea accesului după un număr de accesări eșuate). *Vezi și* Dictionary attack.

Buffer Parte din memoria unui dispozitiv, utilizată pentru stocarea temporară a unor date și informații pentru a fi procesate ulterior.

Buffer overflow Vulnerabilitate prezentă la nivelul codului sursă al unei aplicații ce permite depășirea capacității alocate unui buffer și modificarea memoriei adiacente acestuia. Această vulnerabilitate este folosită pentru a infecta sisteme informatice cu malware. *Vezi și* Buffer.

Bug (Eroare) Termen comun folosit pentru a descrie o greșeală, eroare sau problemă existentă în cadrul codului sursă al unui program sau sistem de operare care poate genera un rezultat eronat, o anomalie sau un efect nedorit.

Bullet Proof Hosting (BPH) Serviciu oferit de deținătorii anumitor domenii web care permite încărcarea și distribuirea, cu restricții minime, de fișiere infectate sau servicii ilegale.

Bus (Local Bus) Componentă hardware, formată din fire, prin intermediul căreia sunt transmise datele între celelalte componente hardware ale unui dispozitiv.

Business Continuity Plan (BCP) Document care descrie modalitatea în care o organizație își disponibilizează produsele și serviciile către clienți în cazul în care au loc diverse evenimente care perturbă sau întrerup funcționarea acestora.

Byte (Octet) Unitatea de bază de stocare a informației în sistemele IT&C. 1 byte e format din 8 biți. *Vezi și* Bit.

C de la Cybercrime-as-a-Service

Cache Memorie specială utilizată pentru stocarea temporară a datelor și care asigură accesul rapid la anumite date utilizate frecvent de procese sau componente ale sistemului.

Cache poisoning Atac cibernetic care constă în înlocuirea datelor (perechi nume domeniu - adresă IP) existente la nivelul memoriei cache a serverelor DNS, cu date ce pot redirecționa utilizatorii către domenii infectate cu software nelegitim. *Vezi și* Cache și Domain Name System (DNS).

Cale de acces (Access Path) Comandă logică care direcționează utilizatorul către locația din dispozitiv în care sunt stocate elementele accesate.

Captcha Metodă automată prin intermediul căreia se determină dacă utilizatorul unui software este o persoană sau un bot. *Exemplu: selectarea imaginilor ce conțin un anumit element.*

Capture the flag Competiție dedicată specialiștilor în securitate cibernetică, care are ca scop identificarea unui șir de caractere cu rol de flag, prin metode specifice (ex. Pen-testing), la nivelul unei rețele sau aplicații. *Vezi și* Pen-testing.

Carrier-sense multiple access with collision detection (CSMA/CD)
Protocol de rețea, utilizat de tehnologia Ethernet, care organizează transmiterea datelor într-un mod eficient la apariția coliziunilor pe canalul de comunicație, pentru a preveni pierderea datelor transmise.

Central Processing Unit (CPU) Componentă hardware a unui sistem IT&C care execută operațiuni aritmetice, logice și de intrare-ieșire indicate de un program de calculator.

Certificat digital Reprezintă echivalentul unui act de identitate în mediul online, care conține autoritatea emitentă, abonatul și perioada de valabilitate operațională, și este utilizat pentru generarea unei semnături electronice. *Vezi și* Semnătură electronică.

Certificare Evaluare completă a măsurilor de securitate de natură tehnică sau non-tehnică ale unui sistem informațional, în cadrul procesului de acreditare, care stabilește în ce măsură un sistem informațional îndeplinește o serie de norme de securitate bine stabilite. *Vezi și* Acreditare și Cerințe de securitate.

Certified Ethical Hacker (CEH) Certificare care atestă faptul că deținătorul are abilități și competențe necesare pentru a identifica vulnerabilități în cadrul unui sistem IT&C, utilizând TTP-uri specifice activității de pen-testing. *Vezi și* Pen-testing.

Chargeware Malware care realizează acțiuni pe dispozitivul infectat prin generarea de costuri victimei și câștiguri atacatorului. *Exemplu: Trimiterea de SMS către un număr cu taxare.*

Cheie privată Dispozitiv sau formulă unică de criptare oferită unui anumit utilizator sau serviciu ca parte dintr-un sistem de criptare asimetrică. *Vezi și* Criptarea asimetrică.

Clickjacking (clickbait) Tehnică ce constă în inducerea în eroare a vizitatorilor unei pagini web prin prezentarea unor elemente de interfață aparent legitime (butoane, imagini, link-uri sau filme) care, prin acționare, pot infecta sau prelua controlul asupra sistemului.

Client Sistem sau proces care adresează solicitări unui server, precum transferul de date către, de la, sau prin intermediul serverului.

Cloud computing Ansamblu distribuit de servicii (servere, capabilități de stocare, aplicații etc.) care se accesează prin intermediul Internetului.

Cloud storage Model de stocare a datelor pe servere virtuale, utilizatorii având acces la datele stocate din orice locație, în condițiile existenței unei conexiuni la rețea.

Cod mașină Reprezentarea internă a secvențelor de cod software specifice fiecărei arhitecturi hardware.

Cod sursa Text scris de programator ce definește funcționalitatea unui program.

Codec Program sau bibliotecă de software, eventual chiar și un echipament hardware, care asigură codarea și decodarea unei informații. Termenul este un acronim format din cuvintele codificare și decodificare.

Codificare Sistem de comunicație în care grupuri arbitrare de litere, numere sau simboluri reprezintă unități de text cu lungime variabilă.

Comand Line Interface (CLI) Interfața prin intermediul căreia utilizatorul transmite comenzi computerului sub forma unor linii de cod.

Common Vulnerabilities and Exposures (CVE) Cod unic asignat pentru fiecare vulnerabilitate a software-urilor public disponibile. Acestea sunt indexate într-o bază de date publică (cve.mitre.org), iar formatul acestora este CVE - anul apariției - numărul asignat. *Exemplu: CVE-2019-1056.*

Compromitere Situație generată ca urmare a dezvăluirii de informații despre un sistem IT&C față de persoane neautorizate, prin încălcarea politicilor de securitate cibernetică, sau prin conferirea de acces neautorizat, modificarea sau distrugerea componentelor sistemului.

Computer forensics Culegerea, identificarea și analiza datelor dintr-un sistem IT&C sau componentă a acestuia, în vederea obținerii de informații în cadrul unor investigații cibernetice (intelligence computer forensics) sau pentru probarea unor infracțiuni în cadrul anchetelor penale.

Computer Network Operations (CNO) Acțiune ofensivă sau defensivă, cu aplicabilitate atât în sfera militară, cât și în cea civilă, derulată cu scopul de a obține superioritate informațională și a discredita adversarii.

Computer Security Incident Response Team (CSIRT) Echipă de reacție formată din specialiști IT cu responsabilități în prevenirea, investigarea, contracararea și limitarea efectelor generate de incidentele de securitate cibernetică.

Confidentiality, Integrity and Availability (CIA) Confidențialitatea, integritatea și disponibilitatea reprezintă cele mai importante cerințe de îndeplinit pentru asigurarea securității cibernetice.
Confidențialitatea - proprietatea unor date și informații de a rămâne cunoscute doar celor care au acest drept și a căror compromitere poate afecta negativ persoane și/sau organizații;
Integritatea - proprietatea unor date, informații și procese de a nu fi modificate sau distruse;
Disponibilitatea - proprietatea unor date, informații, echipamente sau servicii de a putea fi accesate și utilizate, la un anumit moment sau în permanență, fără restricții.

Content Distribution Network (CDN) Sistem de grupare a serverelor, în funcție de criterii geografice, pentru a facilita o transmitere mai rapidă a conținutului pe Internet.

Content Management System (CMS) Un sistem software creat pentru administrarea conținutului unei platforme web, care facilitează organizarea, controlul și publicarea de conținut.

Control Metodă prin care este verificată funcționalitatea un proces sau sistem și în caz de nevoie optimizat sau reparat, pentru a reduce riscul materializării unor amenințări.

Cookie Reprezintă un text special, deseori codificat, trimis de un server către browser-ul web, care este reutilizat de acesta de fiecare dată când navigatorul accesează acel server pe durata unei sesiuni de lucru a unui utilizator.

Counter Antivirus (CAV) Instrument utilizat pentru obfuscarea fișierelor sau aplicațiilor nelegitime în scopul evitării detecției.

Cracker Persoană cu cunoștințe medii și avansate despre domeniul IT&C, care caută și exploatează vulnerabilități la nivelul mecanismelor de protecție de tip DRM. *Vezi și* Digital Rights Management.

Crawling Procesul de colectare și indexare a datelor și informațiilor din conținutul paginilor web cu ajutorul unui bot denumit crawler. Se realizează la scară largă și într-o manieră rafinată, fără a dubla elemente. *Vezi și* Bot și Scraping.

Credențiale Elemente utilizate pentru accesul la informații sau alte resurse din cadrul unui sistem IT&C. În general, termenul se referă la perechi de tip nume de utilizator – parolă. Drept credențiale pot fi utilizate și datele biometrice (amprentele, recunoașterea vocală, scanarea retinei), certificatele digitale etc..

Criminalitate cibernetică/informatică (Cybercrime) Totalitatea faptelor prevăzute de legea penală sau de alte legi speciale care prezintă pericol social și sunt săvârșite cu vinovăție, prin intermediul ori asupra infrastructurilor IT&C.

Criptanaliză Procesul de decriptare și analiză a textului cifrat/criptat. Criptanaliza utilizează formule matematice complexe pentru a identifica vulnerabilități ale algoritmului de criptare cu scopul de a obține informația decriptată/în clar.

Criptare Procesul de codificare a informațiilor, în scopul asigurării securității și confidențialității acestora, precum și prevenirea accesării lor de către utilizatorii neautorizați.

Criptare asimetrică Algoritm de criptare care utilizează o cheie publică și una privată. Expeditorul mesajului criptat va folosi cheia publică a destinatarului pentru a efectua operația de criptare, iar destinatarul va folosi cheia privată pentru a decripta mesajul. Matematic, cele două chei sunt legate, dar cheia privată nu poate fi obținută din cheia publică.

Criptare simetrică Algoritm de criptare care utilizează aceiași cheie, atât pentru criptare, cât și pentru decriptare.

Criptomonedă (Cryptocurrency) Monedă virtuală care utilizează tehnologia blockchain pentru a facilita plăți sigure și cu un grad mare de anonimitate, funcționând independent de sistemul bancar și guvernamental. *Exemple: Bitcoin, Ethereum, Monero etc. Vezi și* Blockchain.

Cross Site Request Forgery (CSRF) Vulnerabilitate prin intermediul căreia un site nelegitim trimite o cerere către o aplicație web la care un utilizator (victimă) este deja autentificat. Cererile nelegitime sunt redirectate către site-ul țintă prin intermediul browser-ului victimei. În acest caz vulnerabilitatea se regăsește în aplicația web țintă și nu în browser-ul victimei și nici în pagina infectată. Nu are ca scop furtul de date, ci determinarea victimelor să modifice informații precum adresa de e-mail, să efectueze transferuri bancare etc. Vulnerabilitatea poate fi exploatată prin atacul cu aceeași denumire.

Cross Site Scripting (XSS) Atac care exploatează o vulnerabilitate ce se regăsește într-o pagină web și care permite unui atacator să introducă linii de cod în paginile web vizitate de alți utilizatori (victime), în scopul obținerii de date cu acces restricționat (Exemplu: credențiale de acces la conturi de e-banking, e-commerce, poștă electronică). Atacul poate fi de două tipuri: XSS persistent și XSS nepersistent.

Cryptojacking Utilizarea neautorizată a resurselor unui alt dispozitiv pentru minarea de criptomonedă. Are loc în momentul în care victima este infectată cu un cod de minare.

Cybercrime-as-a-Service Dezvoltarea și diseminarea ilegală de expertiză, servicii și instrumente (aplicații, rețele de boți, baze de date, servicii infracționale cibernetice etc.), contra cost, către persoane interesate să deruleze atacuri cibernetice. Aceste servicii și instrumente sunt disponibile pe forumuri de criminalitate cibernetică (în general private) din Web și Darkweb.

Cyber-dependent-crime Dezvoltarea și/sau utilizarea de instrumente (tool-uri) complexe în comiterea de atacuri cibernetice cu motivație financiară, care pot avea un impact major asupra securității naționale. În aceste situații, un sistem IT&C este ținta și tot un sistem IT&C constituie și mijlocul prin care se derulează atacul cibernetic.

Cyber-enabled-crime Activități criminale clasice, în derularea cărora este utilizat mediul virtual. *Exemple: carding, skimming etc.*

D de la DDoS

Daemon Program care rulează ca proces de fundal, fără a interacționa cu utilizatorul, cu rolul de a asigura integrarea cu alte programe sau procese cu care este corelat.

Dangling pointer Vulnerabilitate care apare când un obiect este șters sau realocat, fără a se modifica valoarea pointer-ului (în programare, un pointer reprezintă o variabilă care păstrează adresa unei locații de memorie la care sunt stocate date). Astfel, după ștergerea sau realocarea unui obiect din memorie, pointer-ul indică încă locația inițială de memorie. Exploatarea cu succes a vulnerabilității oferă atacatorului posibilitatea de a executa programe nelegitime de la distanță. Vulnerabilitatea poate fi exploatată prin atacul cu aceeași denumire.

Dark web Componentă a mediului Internet care necesită software, configurări și autorizații speciale pentru accesare (ex. browser-ul TOR). Este o componentă a Deep Web-ului, în sensul în care conținutul nu este indexat de motoarele de căutare clasice.

Data hosting Serviciu care oferă hardware-ul, software-ul, sistemele, sistemele de back-up și infrastructura necesară pentru stocarea și accesarea datelor pe o platformă web stabilă.

Data leak Diseminarea intenționată și neautorizată a unor date sau informații cu caracter confidențial către mediul public, astfel încălcându-se principiile *need-to-know* și *need-to-share.*

Data/Information Loss Prevention (DLP/ILP) Termen utilizat pentru a descrie tehnologiile și strategiile utilizate în prevenirea furtului sau pierderii de date/informații.

Data mining Proces complex de analiză statistică și logică a unor volume mari de date prin care se urmărește identificarea informațiilor relevante și a unor pattern-uri.

Data spill Diseminarea accidentală și neautorizată a unor date sau informații cu caracter confidențial către mediul public, astfel încălcându-se principiile *need-to-know* și *need-to-share.*

Date biometrice Atribute și caracteristici fizice ale unei persoane care sunt utilizate pentru procesul de autentificare. *Exemple: retina, amprenta, forma feței etc.*

Deep web Componentă a mediului World Wide Web care nu este indexată de motoarele tradiționale de căutare sau directoarele de resurse, paginile web putând fi accesate exclusiv prin intermediul unor mijloace specifice (ex. browser-ul TOR). Adresele paginilor web sunt caracterizate prin caractere alfaseminumerice (literele alfabetului și cifrele de la 2 la 7), și prin extensii specifice (ex. onion).

Defacement Atac asupra unui website care constă în înlocuirea neautorizată a interfeței paginii web prin exploatarea unor vulnerabilități de securitate cibernetică. Elementele grafice introduse pot conține mesaje prin care se motivează atacul, autorul sau gruparea care a efectuat atacul, alte date compromise (precum conturi de utilizator și parole) sau eventuale link-uri către alte site-uri. În urma unui atac de tip defacement, forma legitimă a site-ului web este inaccesibilă, fiind necesară restaurarea lui, precum și verificarea breșelor de securitate care au permis atacul.

Demilitarized zone (DMZ) Arhitectură conceptuală de rețea în care serverele cu acces public sunt plasate separat pe un segment izolat de rețea. Scopul DMZ este acela de a asigura că serverele accesibile publicului nu pot intra în contact cu alte segmente interne de rețea, în situația în care un server este compromis.

Denial of Service (DoS) Atac prin care se urmărește indisponibilizarea, blocarea sau epuizarea resurselor unui sistem IT&C, rețea sau componentă a acesteia prin „saturarea" țintei cu solicitări de comunicare externe, astfel încât acesta să nu mai poată reacționa eficient la traficul legitim, devenind indisponibilă. De obicei, un atac de tip DoS utilizează un singur sistem IT&C și o singură conexiune la Internet.

Dictionary attack Atac cibernetic de tip *brute force* care urmărește accesarea neautorizată a unor resurse sau sisteme IT&C, prin încercarea succesivă a parolelor sau cheilor de decriptare aflate într-o listă predefinită de cuvinte sau fraze. *Vezi și* Brute force attack.

Digital Rights Management (DRM) Serie de tehnologii utilizate pentru a proteja drepturile de autor ale produselor software și multimedia.

Directory harvest attack Metodă de atac folosită pentru a determina adresele de e-mail valide care aparțin unui domeniu, prin folosirea tehnicii de brute force. Concret, atacatorul utilizează un program care încearcă toate combinațiile posibile de caractere utilizate în adresele de e-mail.

Distributed Denial of Service (DDoS) Atac prin care se urmărește indisponibilizarea, blocarea sau epuizarea resurselor unei rețele sau unui sistem IT&C, de obicei prin intermediul unui botnet. În cadrul atacului sunt folosite dispozitive infectate (botnet-ul) pentru a transmite cereri către sistemul țintă. Eficiența unui astfel de atac sporește considerabil în momentul în care sunt folosite cât mai multe dispozitive de pe care se lansează simultan cereri către sistemul țintă. *High Orbit Ion Cannon (HOIC) și Low Orbit Ion Cannon (LOIC)* sunt două exemple de aplicații folosite în derularea de atacuri DDoS, care nu necesită cunoștințe avansate pentru a fi utilizate.

Distributed Ledger Technology (DLT) Sistem digital de înregistrare a tranzacțiilor (valută, bunuri, date etc.) și a detaliilor despre acestea în mai multe locații simultan. Spre deosebire de bazele de date clasice, DLT nu are o bază de date centrală sau un administrator.

DNS attack Gamă de atacuri cibernetice care exploatează vulnerabilități ale serverului DNS și au ca efect indisponibilizarea acestuia. Cele mai cunoscute tipuri de atacuri sunt *DoS, DDoS* și *cache poisoning.*

Domain Name System (DNS) Protocol utilizat pentru localizarea numelor domeniilor din Internet și translatarea lor în adrese IP. *Vezi și* DNS attack și Adresă IP.

Download (Descărcare) Copierea fișierelor din server în calculatorul clientului. Doxing Tehnică ce constă în obținerea și postarea pe Internet a informațiilor sensibile cu caracter personal (credențiale, coduri personale, numere de telefon, funcții deținute, informații despre carduri de credit, adrese, pseudonime etc.). Metoda este folosită, de regulă, de către grupări cu motivație ideologică (hacktivism sau terorism) în scopul extragerii și expunerii datelor personale/ profesionale care aparțin angajaților din instituții publice sau companii internaționale.

Doxing Tehnică ce constă în obținerea și postarea pe Internet a informațiilor sensibile cu caracter personal (credențiale, coduri personale, numere de telefon, funcții deținute, informații despre carduri de credit, adrese, pseudonime etc.). Metoda este folosită, de regulă, de către grupări cu motivație ideologic (hacktivism sau terorism) în scopul extragerii și expunerii datelor personale/profesionale care aparțin angajaților din instituții publice sau companii internaționale.

E de la Exploit

E-Government Utilizarea tehnologiilor și aplicațiilor IT&C în activitatea instituțiilor publice cu scopul de a eficientiza actul de guvernare.

End-to-end encryption (E2EE) Sistem de comunicare care criptează datele transmise pe tot parcursul transmiterii acestora și în cadrul căruia doar utilizatorii finali dețin cheile de decriptare.

Ethernet Tehnologie care se aplică în rețele de tip LAN (Local Area Network) și este utilizată pentru asigurarea traficului de date, prin folosirea unui protocol de tip CSMA/CD.

Ethical hacking Proces legitim, derulat de *white hat hackers*, de identificare a vulnerabilităților și riscurilor din cadrul unui sistem IT&C, cu scopul de a le remedia și preveni o eventuală exploatare a acestora în scopuri nelegitime.

Evaluarea vulnerabilității Examinare sistematică a unui sistem sau produs informațional pentru a determina nivelul existent de securitate, a identifica măsurile ce se impun, în vederea aducerii sistemului la conformitate cu standardele de securitate existente.

Exploit Un software sau o secvență de cod care exploatează vulnerabilități ale sistemelor IT&C (ex. sisteme de operare/aplicații), în scopul compromiterii acestora.

F de la Firewall

False flag Acțiune concepută și derulată pentru a induce în eroare entități interesate, astfel încât să pară a fi efectuată de altă entitate și/sau în alt scop decât cel real.

File Transfer Protocol (FTP) Protocol standard de rețea, utilizat pentru transferul de fișiere între un client și un server dintr-o rețea de calculatoare.

Firewall Sistem (hardware sau software) proiectat cu scopul de a proteja un calculator sau rețea internă (privată) de accesul neautorizat din exterior, prin implementarea unor politici de securitate, prin care sunt filtrate cererile și sunt respinse cele care nu respectă criteriile specificate.

Firmware Programe și date stocate, de regulă, la nivelul memoriei nevolatile, care nu pot fi scrise sau modificate prin procedee uzuale și care au rolul de a asigura funcționarea componentelor hardware.

Flooding Atac cibernetic care compromite disponibilitatea unui sistem IT&C prin transmiterea unui flux supradimensionat de input-uri sau pachete de date de dimensiuni mari, care nu pot fi procesate de acel sistem. Acest atac este similar celui de tip DoS.

Fork Bomb (Wabbit/Rabbit virus) Atac de tip *denial of service* în care un program se multiplică continuu astfel încât resursele sistemului vizat sunt indisponibilizate, blocate sau epuizate. *Vezi și* Denial of Service.

Freeware Aplicație, program sau software disponibile online pentru utilizarea gratuită.

Full Disk Encryption (FDE) Tehnologie de criptare a informației pe un disk drive prin intermediul unui software sau hardware.

Full Path Disclosure (FPD) Vulnerabilitate ce conferă execuția unor scripturi SQL în lansarea unor atacuri de tip SQL Injection.

Furt de identitate Obținerea și utilizarea fără drept a credențialelor sau elementelor de autentificare ale altei persoane, pentru a obține acces neautorizat la un sistem sau infrastructură IT&C.

G de la Gateway

Gateway Dispozitiv IT&C care facilitează conexiunea unui host la o rețea. Un exemplu de dispozitiv gateway este router-ul.

Graphical User Interface (GUI) Interfață grafică prin intermediul căreia utilizatorul interacționează cu dispozitivele. Nu utilizează interfață cu linii de cod.

H de la Hacker

Hacker Specialist IT care caută și exploatează vulnerabilități ale sistemelor IT&C. Aceștia pot fi clasificați în trei categorii:
Black Hat - a căror motivație implică derularea unor acțiuni ilegale;
White Hat - a căror motivație implică derularea unor acțiuni autorizate;
Gray Hat - a căror motivație implică atât derularea unor acțiuni autorizate, cât și ilegale.

Hacktivist Hacker care realizează atacuri cibernetice cu scopul de a transmite mesaje de protest, în contextul unui eveniment politic, social sau economic.

Hardening Proces de securizare a unui sistem IT&C prin simplificarea funcțiilor pe care le îndeplinește și implicit prin reducerea riscului de apariție a vulnerabilităților.

Hardware Componentele fizice ce alcătuiesc un sistem IT&C. *Exemple: placă de bază, placă video, memorie, DVD-ROM, tastatură, ecran etc.*

Hash Funcție matematică bazată pe algoritmi specializați care generează un cod fix și unic pe baza caracterelor introduse. Rezultatul nu poate fi inversat pentru a obține datele originale, dar datele identice au hash identic. Funcție care poate fi utilizată de servere pentru stocarea parolelor de acces ale utilizatorilor. Tipuri de hash: SHA-1, MD5 etc.

Header Informație suplimentară, situată la începutul unui set de date, necesară descrierii și procesării acestuia.

Hijacking Tip de atac în care atacatorul preia controlul unei comunicații dintre două entități cu scopul de a obține acces neautorizat. *Vezi și* Furt de identitate.

Honeypot Resursă IT&C a cărei caracteristică constă în faptul că poate fi testată, atacată sau compromisă, în scopul identificării unor elemente de modus operandi ale unui atacator cibernetic. Această resursă poate fi reprezentată de un server, o stație, un router, o adresă de email publicată pe un site etc.

Hop point O porțiune a căii dintre sursă și destinație într-o comunicație între două sisteme IT&C.

Host/end device Orice dispozitiv IT&C conectat la o rețea.

Hostname Nume asignat unui dispozitiv IT&C pentru identificarea acestuia în cadrul unei rețele.

Hub Dispozitiv utilizat în cadrul unei rețele ca punct de conexiune comun pentru alte dispozitive.

Hyper Text Markup Language (HTML) Limbaj principal utilizat pentru crearea și afișarea paginilor web.

Hyper Text Transfer Protocol (HTTP) Protocol care asigură uniformitatea schimbului de informații la nivelul World Wide Web.

Hyper Text Transfer Protocol Header Injection Vulnerabilitate ce permite atacatorilor să distribuie, prin multiplicare, un răspuns HTTP care are injectat cod nelegitim.

Hyper Text Transfer Protocol/Secure (HTTPS) Protocol HTTP folosit pentru comunicații securizate, care presupune suprapunerea protocolului tradițional HTTP peste protocolul de securitate TLS (Transport Layer Security).

Identificare Acțiune sau proces de recunoaștere a unei entități (utilizator, proces sau dispozitiv) într-un sistem și distingerea acesteia de oricare altă entitate prin intermediul unui set de valori/caracteristici.

Incident de securitate cibernetică Eveniment survenit în spațiul cibernetic ale cărui consecințe afectează securitatea cibernetică.

Incident Response Concept folosit în domeniul securității cibernetice prin care sunt definite metodele și tehnicile folosite în cadrul organizației pentru gestionarea activităților în cazul unui atac cibernetic.

Indicators of Compromise (IoC) Date sau informații identificate în cadrul unui sistem IT&C, ce indică faptul că a avut loc un atac cibernetic care a compromis sistemul sau rețeaua.

Information Security (InfoSec) Protecția informației și a sistemelor IT&C împotriva accesului, utilizării, dezvăluirii, perturbării, modificării, înregistrării sau distrugerii de către persoane neautorizate, în scopul asigurării confidențialității, integrității și disponibilității acestora. *Vezi și* Confidentiality, Integrity and Availability (CIA).

Information Technology and Communications (IT&C) Tehnologia informației și comunicațiilor reprezintă ansamblul de echipamente hardware și software interconectate, care asigură prelucrarea (obținerea, procesarea, stocarea, convertirea, afișarea, controlul și transmiterea) informației.

Info-stealer Malware creat cu scopul de a extrage date și informații din sistemul țintă. Două exemple de info-stealer sunt Gozi și Gauss, care au fost create cu scop de a sustrage date și informații bancare accesibile online (nume de utilizatori, parole, numere de conturi) aparținând persoanelor fizice sau companiilor, pe care le transmit ulterior către servere de comandă și control.

Infrastructură cibernetică critică Infrastructură IT&C, constând în sisteme informatice, aplicații aferente, rețele și servicii de comunicații electronice, care deservește un sector vital al unui stat și a cărei incapacitate de funcționare sau distrugere este de natură a crea efecte majore asupra securității naționale.

Inginerie socială (Social engineering) Acțiuni de manipulare a factorului uman, în vederea atingerii unor etape intermediare (obținerea de credențiale, accesarea unui fișier infectat, transmiterea unor sume de bani) necesare derulării unor atacuri cibernetice.

Instant messaging (IM) Sistem de comunicații de tip chat online, care asigură transmiterea de mesaje text sau multimedia în timp real.

Inteligența artificială Domeniu IT&C care urmărește conceperea, crearea și operaționalizarea unor instrumente care au capacitatea de a realiza sarcini asociate în mod tradițional unei ființe umane.

International Mobile Subscriber Identity (IMSI) Număr unic de identificare al utilizatorilor unei rețele de telefonie mobilă.

Internet Control Message Protocol (ICMP) Protocol de comunicație utilizat în cadrul rețelelor de comunicație pentru a indica disponibilitatea unui sistem de calcul.

Internet Message Access Protocol (IMAP) Protocol standard utilizat de un client de e-mail (program utilizat pentru gestionarea unui cont de poștă electronică) pentru accesarea mesajelor e-mail din folderele aflate pe un server.

Internet of Things (IoT) Concept care se referă la interconectarea tuturor dispozitivelor, sistemelor și serviciilor din sfera IT&C prin intermediul Internetului.

Internet Protocol (IP) Protocol de comunicații folosit pentru transmiterea de date între dispozitive prin intermediul rețelelor de comunicații și sistemelor interconectate ale unor asemenea rețele. *Vezi și* Adresă IP.

Internet Protocol Security (IPsec) Set de protocoale folosite la securizarea comunicațiilor prin autentificarea și criptarea fiecărui pachet IP al unei sesiuni de comunicații.

Internet Relay Chat (IRC) Protocol utilizat pentru mesagerie text în timp real (chat), prin Internet sau pentru servicii sincrone de conferință. Servește pentru comunicații de grup în forumuri de discuții (canale), permite realizarea de comunicații de tip unu-la-unu (prin mesaje private, chat și transfer de date), precum și partajarea de fișiere.

Internet Relay Chat daemon (IRCd) Software în cadrul serverului care implementează protocolul IRC. *Vezi și* Internet Relay Chat și Daemon.

Internet Service Provider (ISP) Furnizor de servicii Internet care oferă conexiune și acces la Internet.

Intrusion Detection System (IDS) Sistem care culege și analizează informații din diferite zone ale unei rețele, cu rol de a identifica posibilele activități intruzive, fără a le bloca.

Intrusion Prevention System (IPS) Sistem care poate detecta o activitate intruzivă și care încearcă să oprească o asemenea activitate înainte ca aceasta să-și atingă ținta și să producă efecte.

Intruziune Acțiunea neautorizată de accesare a unei resurse IT&C prin ocolirea mecanismelor de securitate cibernetică.

IP flood Atac de tip DoS prin care sistemul țintă nu mai poate fi accesat de utilizatori legitimi din cauza traficului intens care blochează lățimea de bandă. *Vezi și* Bandwidth și Denial of Service.

IP spoofing Tehnică de falsificare a adresei IP sursă pentru a masca identitatea atacatorului. *Vezi și* Adresă IP și Denial of Service.

IRC bouncer Serviciu care oferă o conexiune de tip proxy și păstrează clientul conectat la rețea chiar dacă acesta nu este online.

J de la Java

Jailbreak Înlăturarea restricțiilor de securitate impuse de producător unui dispozitiv (de obicei telefon mobil).

Jamming Atac prin care se încearcă bruiajul și interferența cu transmisiile realizate prin unde radio, blocând accesul utilizatorilor autorizați.

Java Limbaj de programare utilizat pentru conceperea unor aplicații software pe platforme multiple.

JavaScript Limbaj de programare folosit preponderent pentru construirea și introducerea unor funcționalități la nivelul paginilor web.

K de la Keylogger

Kernel (Core) Centru vital al unui sistem de operare, care asigură serviciile de bază pentru toate componentele unui dispozitiv.

Keykatcher Dispozitiv de legătură care se conectează între tastatură și unitatea centrală a calculatorului. Acesta poate captura și stoca aproximativ două milioane de caractere, introduse prin intermediul tastaturii, într-un format codat.

Keylogger Software care monitorizează și înregistrează ceea ce se introduce de la tastatură pe un dispozitiv IT.

Kill switch Mecanism încorporat în software, utilizat pentru închiderea sau întreruperea activității, în caz de urgență/necesitate, a unui dispozitiv infectat.

Killermobile Aplicație care se instalează pe telefonul interceptat, ulterior controlul fiind realizat cu ajutorul unui alt telefon care interceptează și trimite comenzi de configurare prin SMS.

Lateral movement (Mișcare laterală) Etapă din cadrul unui atac cibernetic ce presupune tehnici și metode utilizate de un atacator pentru a se propaga în cadrul rețelei.

Limbaj de programare Set bine definit de expresii și reguli valide, utilizate în dezvoltarea aplicațiilor. *Exemple: C, Java, Python, Pearl, Pascal etc.*

Link *Vezi* Uniform Resource Identifier (URI).

Local Area Network (LAN) Tip de rețea care interconectează dispozitive aflate pe o zonă geografică restrânsă. *Exemplu: rețeaua unei organizații.*

Local File Inclusion (LFI) Vulnerabilitate prezentă la nivelul aplicațiilor web care permite unui atacator executarea de coduri nelegitime.

Log Fișier cu istoricul înregistrărilor din cadrul unui sistem sau rețea. Aceasta poate conține date despre activități precum accesarea sistemului și crearea de fișiere.

Login Bypass Tehnică prin care un atacator, profitând de un defect de implementare, poate ocoli mecanismele de securitate pentru a obține acces neautorizat la un sistem IT&C sau rețea.

M de la Malware

Managementul riscului (Risk management) Un proces complex, continuu și flexibil de identificare, evaluare și contracarare a riscurilor la adresa securității cibernetice, bazat pe utilizarea unor tehnici și instrumente complexe, pentru prevenirea pierderilor de orice natură.

Mașină virtuală Aplicație software care simulează în totalitate funcționarea componentelor hardware din componența unui sistem IT&C (computer). Utilizatorul poate specifica arhitectura hardware (32 sau 64 de biți), capacitatea memoriei RAM și a HDD-ului, frecvența și numărul de nuclee ale procesorului sau numărul de porturi și interfețe. Mașinile virtuale sunt create și simulate cu ajutorul unor aplicații software specializate (ex. VmWare, Virtual PC și Sun Virtual Box) care se implementează pe un sistem de operare (Windows, Linux etc.).

Malvertising Acțiune ce constă în injectarea cu cod nelegitim a unor bannere publicitare sau site-uri de publicitate și care determină modificarea adresei paginii web cu o nouă adresă web infectată pentru a răspândi malware.

Malware (malicious software) Software realizat pentru a îndeplini scopuri nelegitime în momentul în care accesează un dispozitiv, rețea sau sistem IT&C, fără acordul sau cunoștința proprietarului. *Exemple: troian, virus, vierme, spyware, backdoor etc.*

Malware polimorf Malware care își schimbă atributele pentru a evita detecția de către un program anti-malware. Acest proces este automat, sens în care funcțiile software-ului se păstrează, dar metoda de operare, locația și alte atribute se pot schimba.

Man in the middle O formă de interceptare în care atacatorul se interpune într-o comunicație privată sau un schimb de date privat și are posibilitatea de a accesa sau modifica conținutul acesteia.

Maparea rețelei (Network mapping) Efectuarea de operațiuni electronice de inventariere a dispozitivelor (ex. server, router, stație, switch) și serviciilor (ex. email) dintr-o rețea.

Master Boot Record (MBR) Componentă a mediului de stocare de pe un dispozitiv IT&C, care facilitează încărcarea/pornirea sistemului de operare.

Media Access Control (MAC) Cod unic obligatoriu, asignat de către producător, folosit pentru identificarea unui sistem sau dispozitiv.

Memorie externă Partea memoriei formată din dispozitive de stocare a cantităților mari de date. *Exemple: Hard disk extern sau USB stick.*

Memorie internă Parte a memoriei care intră în contact direct cu microprocesorul, prin intermediul căreia se pot aprecia performanțele unui computer. Este unitatea funcțională destinată păstrării permanente sau temporare a programelor și datelor necesare utilizării sistemului de operare. Este formată din două tipuri de memorie: RAM și ROM. *Vezi și* Random Access Memory și Read Only Memory.

Mentenanță Ansamblu de activități tehnico-organizatorice care au ca scop menținerea sau restabilirea unui echipament într-o stare specifică pentru ca acesta să fie în măsura de a asigura un serviciu.

Metadate Date care caracterizează un pachet de date.

Metaverse Spațiu colectiv care îmbină realitatea cu lumea virtuală pentru a genera un univers digital. *Vezi și* Realitate augmentată și Realitate virtuală.

Minarea de criptomonedă (Cryptomining) Generarea de monede virtuale prin utilizarea puterii de calcul pentru a rezolva probleme matematice complicate.

Mobile Remote Acces Tool (Mobile RAT) Aplicație care permite controlul de la distanță al dispozitivelor portabile (telefon, smartphone, tabletă etc.) și obținerea accesului la resursele dispozitivului. Instalarea acestor programe se poate face de la distanță. *Vezi și* Remote Acces Tool.

Monitorizarea comportamentului (Behavior monitoring) Metodă de supraveghere utilizată pentru a identifica intenții nelegitime de accesare sau executare de programe. Scopul acestei metode este de a alerta rapid administratorul în momentul detectării unui potențial risc.

Multiplexare Metodă prin care mai multe semnale analogice sau fluxuri de date digitale sunt combinate într-un singur semnal și transmise prin intermediul unui singur canal.

N de la Network scanning

Near Field Communication (NFC) Tehnologie ce utilizează frecvențe radio pentru a permite dispozitivelor să comunice între ele prin atingere sau apropiere, la o distanță mai mică de 10 cm. Pentru a funcționa, ambele dispozitive trebuie să dețină un cip NFC.

Network Attached Storage (NAS) Dispozitiv care oferă utilizatorilor din cadrul unei rețele un spațiu centralizat de stocare.

Network Address Translation (NAT) Mecanism de translatare a adreselor IP private (nu sunt accesibile din Internet) în adrese IP publice (accesibile în Internet). Se bazează pe existența unei tabele de translatare.

Network forensics Procesul de captare, înregistrare și analiză a informațiilor și evenimentelor din cadrul unei rețele pentru a identifica indiciile unui atac cibernetic.

Network Level Authentification (NLA) Tehnologie utilizată în cadrul protocolului RDC care solicită autentificarea utilizatorului înaintea stabilirii unei sesiuni cu serverul.

Network recording Procesul de copiere și stocare a unei copii a tuturor datelor transmise în cadrul unei rețele, într-o perioadă de timp prestabilită.

Network scanning Proces de identificare a dispozitivelor dintr-o rețea și a serviciilor care rulează pe acestea. Activitatea de scanare este o practică des întâlnită în Internet, fiind în general o etapă premergătoare unui atac cibernetic, întrucât ajută la colectarea de informații despre sistem, care pot evidenția anumite servicii vulnerabile.

Network segmentation Tehnică aplicată rețelelor de dimensiuni mari, care constă în împărțirea acestora în secțiuni mai mici. Prin implementarea unor politici de securitate subsumate acestui principiu se poate realiza o mai bună administrare și protecție a rețelei.

Nonrepudiere Capacitatea unui sistem de a certifica/confirma transmiterea nemodificată a unui mesaj de către un utilizator.

Obfuscare Procedeu de scriere a codului, în dezvoltarea unui software, care îl face greu de înțeles, descifrat și analizat.

Open Source Intelligence (OSINT) Procesul de colectare și analiză a datelor și informațiilor din surse publice, în contextul realizării unor materiale de intelligence.

Outsourcing (Externalizare) Încredințarea sau delegarea unor activități către firme specializate dintr-un anumit domeniu.

P de la Pen-testing

Packet Pachet de date care este transmis prin intermediul unei rețele.

Packet filtering Tehnică firewall utilizată pentru a controla fluxul de pachete de date (packets) care intră și ies dintr-o rețea.

Packet sniffer Dispozitiv sau software ce permite monitorizarea și înregistrarea traficului de rețea.

Pagină web (Web page) Resursă aflată în spațiul web, în format HTML, care se poate afișa pe monitorul computerului.

Parolă (password) Un șir de caractere (litere, cifre și/sau caractere speciale) secret, cu rol de protecție, folosit (de regulă împreună cu un nume de utilizator) la autentificarea sau obținerea accesului autorizat la anumite dispozitive, sisteme, servicii sau date.

Partajarea fișierelor (File sharing) Procedeu prin care date publice sau private (documente, aplicații, fișiere multimedia etc.) sunt puse la dispoziție și pot fi accesate în cadrul uneia sau mai multor rețele, cu diferite nivele de acces din partea utilizatorilor acesteia.

Partiție Diviziune a capacității de stocare a unui hard-disk.

Passfile Dicționar cu cele mai comune și utilizate credențiale (nume de utilizator și parole). *Vezi și* Credențiale.

Password sniffing Tehnică folosită la nivelul site-urilor și aplicațiilor web cu scopul de a identifica credențialele unui utilizator.

Password spraying Metodă de atac utilizată pentru obținerea accesului neautorizat la un număr mare de conturi, prin încercarea unei parole cu un grad scăzut de securizare (ex. 1234, 0000, admin etc.).

Patch (Update) Actualizarea unui software în vederea înlăturării unor defecțiuni/vulnerabilități anterioare, cât și optimizării unor funcții.

Patching (Updating) Procesul de actualizare a unei aplicații software cu o versiune îmbunătățită de către dezvoltatorul acesteia.

Peer-to-peer (P2P) Model de arhitectură a rețelei care permite utilizatorilor să partajeze fișiere, fără a le stoca sau descărca din serverul central.

Pen-testing (test de penetrare) Metodologie de testare a securității unei infrastructuri cibernetice, prin simularea unui atac din exteriorul și / sau interiorul acesteia, în vederea stabilirii potențialelor vulnerabilități și măsurilor necesare îmbunătățirii nivelului de securitate.

Payload Componenta software-ului nelegitim care îndeplinește funcția pentru care a fost creat (ex. ștergerea, criptarea sau transmiterea datelor).

Persistență Modalitatea prin care un software nelegitim își păstrează existența și activitatea în cadrul unui sistem IT&C, ulterior măsurilor întreprinse pentru a fi identificat și eliminat.

Personal Area Network (PAN) Rețea de mici dimensiuni utilizată pentru interconectarea dispozitivelor utilizate de o persoană.

Perturbare Eveniment care provoacă disfuncții la nivelul sistemului IT&C sau chiar indisponibilizarea acestuia.

Pharming Atac prin care se urmărește redirecționarea unui utilizator care accesează un site legitim către un site nelegitim. Se realizează prin modificarea host-urilor de pe computerul vizat sau prin exploatarea unei vulnerabilități în software-ul serverului DNS, fără consimțământul victimei.

Phishing Reprezintă o formă de activitate infracțională ce are ca scop obținerea unor date confidențiale, cum ar fi credențiale (pentru aplicații de tip Internet banking, aplicații de comerț electronic, carduri de credit etc.) prin folosirea tehnicii de inginerie socială. Se realizează prin intermediul mail-ului sau prin clonarea site-urilor și, ulterior, transmiterea de solicitări clienților referitoare la datele conturilor personale. *Vezi și* Spear phishing, Vishing și Smishing.

Php: Hypertexted Preprocessor (PHP) Limbaj de programare folosit pentru dezvoltarea paginilor și aplicațiilor web.

Ping of death attack Atac, de tip DoS/DDoS, ce constă în transmiterea unui pachet de date mai mare decât memoria buffer a plăcii de rețea din sistemul IT&C țintă, generând astfel blocarea acestuia. *Vezi și* Distributed Denial of Service și Denial of Service.

Pivoting Metodă utilizată în pen-testing și atacuri cibernetice pentru a facilita propagarea dintr-un sistem compromis în alt sistem sau rețea. *Vezi și* Pen-testing.

Platform as a Service (PaaS) Serviciu de tip cloud care pune la dispoziție utilizatorilor o platformă de tip *cloud computing* pentru dezvoltarea, rularea și administrarea aplicațiilor.

Port (în rețea) Parte a adresei de rețea de calculatoare care determină atribuirea conexiunilor TCP/UDP, a pachetelor de date către servere și clienți.

Port hardware Componentă care permite conectarea fizică a unui dispozitiv la un alt dispozitiv sau la o rețea.

Port software Construcție software care servește ca punct de comunicație în cadrul sistemului de operare al computerului respectiv.

Port scan Metodă de scanare a unui sistem dintr-o rețea, utilizată în vederea identificării porturilor deschise și a serviciilor disponibile pe acesta.

Portofel electronic/digital (Wallet) Instrument de plată rapid și anonim în cadrul unei platforme digitale.

Potentially Unwanted Program (PUP) Tip de software pe care utilizatorul a acceptat să îl descarce, dar care realizează sau facilitează funcții nelegitime.

Privilegiu Drept de citire, scriere, ștergere sau execuție conferit unei persoane sau proces în cadrul unui sistem.

Programmable Logic Controllers (PLC) Computer industrial proiectat pentru a funcționa în condiții nefavorabile (vibrații puternice, praf etc.)

Protocol Set de reguli și reglementări ce determină modalitatea în care datele sunt transmise în cadrul comunicațiilor prin intermediul rețelelor de calculatoare. *Exemple: IP, HTTPS, FTP, TCP, BGP DHCP etc.*

Proxy server Server intermediar care asigură redirecționarea traficului între computer și Internet, cu scopul de a anonimiza adresele reale de la care se conectează utilizatorul și a securiza conexiunea. *Vezi și* Virtual Private Network.

Pushed shell Linie de comandă trimisă atacatorului de către calculatorul infectat.

Q de la Quarantine

Quantum Key Distribution (QKD) Metodă de comunicare securizată pe baza unui protocol criptografic.

Quarantine Procesul de izolare a unui malware pentru a nu cauza viitoare daune sistemului IT&C sau datelor stocate pe acesta. De obicei, este etapa premergătoare eliminării sau examinării malware-ului.

R de la Ransomware

Rainbow tables Bază de date sau set de valori criptate care pot fi folosite pentru a obține valorile inițiale, în cazul în care au fost asociate anterior. De exemplu, valorile hash pot fi introduse într-un motor de căutare pentru a obține valorile inițiale, înainte de criptarea acestora.

Random Access Memory (RAM) Reprezintă memoria principală a unui dispozitiv, în care sunt stocate codul, datele și programele folosite de procesor. Are caracter volatil, iar la oprirea dispozitivului conținutul memoriei RAM este pierdut.

Ransomware Software nelegitim care restricționează accesul și utilizarea dispozitivului, prin criptarea conținutului, până când este plătită o recompensă. *WannaCry (WannaCrypt)* este un exemplu de atac cibernetic derulat în mai 2017 la nivel mondial, care a utilizat un ransomware pentru a exploata o vulnerabilitate a sistemului de operare Microsoft Windows și a cripta fișierele calculatorului infectat, cerând o răscumpărare pentru a le decripta.

Ransomware-as-a-service Serviciu în mediul online, pe forumuri de criminalitate cibernetică și Darkweb, care pune la dispoziție programe ransomware făcute la comandă, în schimbul unor sume de bani, pentru derularea de atacuri cibernetice.

Read Only Memory (ROM) Componentă a memoriei interne, cu caracter nevolatil, unde sunt stocate datele înscrise de producătorul computerului în momentul fabricării. Este în general utilizată pentru a stoca BIOS-ul. *Vezi și* Basic Imput Output System.

Realitate augmentată Mediu real în care sunt proiectate prin intermediul unor lentile (camere foto/video sau ochelari) elemente digitale (imagini, locații, mesaje text etc.) care au impact doar asupra utilizatorului. *Vezi și* Metaverse și Realitate virtuală.

Realitate virtuală (Virtual reality) Mediu artificial, generat cu ajutorul unui computer, pentru a replica aspecte din realitate. *Vezi și* Metaverse și Realitate augmentată.

Reconnaissance Etapă incipientă a unui atac cibernetic care are ca scop obținerea de informații despre sistemului țintă și vulnerabilitățile acestuia.

Recovery time objective (RTO) Timpul alocat de administratorul unui sistem sau infrastructură IT&C pentru reabilitare în cazul unui atac cibernetic.

Red Team Echipă formată din persoane care au rolul de a ataca sistemele informatice protejate de echipa de apărători (Blue Team), în cadrul unui concurs de hacking, în conformitate cu un set de reguli stabilite și cu monitorizare din partea unui grup neutru, cu rol de arbitru (White Team). *Vezi și* Blue Team și White Team.

Redundanță Alocarea unui excedent de resurse care deservesc aceeași funcție în cadrul unui sistem IT&C pentru a se înlocui reciproc în cazul unui eveniment de securitate cibernetică care ar afecta funcționalitatea acestuia.

Reflecting (non-persistent) cross-site scripting Vulnerabilitate a aplicațiilor web care afectează utilizatorii individuali prin rularea unui cod sau program în urma accesării unui link infectat cu malware.

Remote access *Vezi* Acces de la distanță.

Remote Access Tool/Trojan (RAT) Aplicație malware care permite controlul de la distanță al dispozitivelor și obținerea accesului la resursele dispozitivului. Instalarea acestor programe se poate face de la distanță, prin accesarea unei pagini web infectate. *Vezi și Mobile Remote Acces Tool.*

Remote Code Execution (RCE) Vulnerabilitate ce conferă posibilitatea unui atacator de a executa, de la distanță, comenzi la nivelul sistemului de operare sau al unei aplicații, cu diferite privilegii.

Remote Desktop Connection (RDC) Tehnologie care permite unui computer local să se conecteze și să controleze de la distanță un computer din rețea sau din Internet. O soluție software care poate fi folosită pentru controlul de la distanță a unui computer sau pentru colaborarea în cadrul unei echipe este Team Viewer.

Remote Desktop Protocol (RDP) Protocol de comunicații în cadrul unei rețele, conceput pentru accesul și gestionarea calculatoarelor de la distanță.

Remote File Inclusion (RFI) Vulnerabilitate ce permite includerea unui fișier aflat pe alt server, folosind un parametru de tip GET. Practic, scriptul va include direct fișierul specificat prin valoarea unei variabile trimise prin parametrul GET. Vizează furtul de informații și compromiterea serverelor.

Remote Terminal Unit (RTU) Dispozitiv electronic utilizat in cadrul sistemelor de control industrial (SCADA). *Vezi și* SCADA.

Replay attack Atac care constă în captarea unei informații transmise (autentificare, informație de control, date despre transferuri bancare etc.) și retransmiterea sa ulterioară fără a fi detectată existența unei interferențe în proces.

Rețea (Network) Grup de dispozitive (routere, hub-uri, controlere de telecomunicații etc.) interconectate, care comunică prin intermediul unor protocoale specifice.

Rețea externă (Extranet) Rețea care folosește tehnologia World Wide Web și permite partajarea de date sau operațiuni ale unei organizații cu furnizori, parteneri, clienți sau alte entități.

Rețea internă (Intranet) Rețea care aparține unei organizații și este utilizată exclusiv de membrii acesteia.

Reziliența infrastructurilor cibernetice Capacitatea componentelor infrastructurilor cibernetice de a rezista unui incident sau atac cibernetic și de a reveni la starea de normalitate.

Risk register Registru care conține o listă cu potențialele pierderi sau daune la care sistemul este expus.

Rivest-Shamir-Adleman (RSA) Algoritm de criptare cu chei publice, fiind primul algoritm utilizat atât pentru criptare, cât si pentru semnătura electronică. A fost publicat în 1978 și poartă numele celor trei autori.

Root Utilizatorul sau contul cu cel mai înalt nivel într-un sistem de tip UNIX, care are acces la toate comenzile și fișierele din sistem.

Rootkit Aplicație malware nedetectabilă realizată pentru a obține acces și control asupra nucleului (core/root), ascunzând existența unor procese sau programe de metodele normale de detecție și preluare a accesului asupra resurselor sistemului.

Router Dispozitiv care permite transmiterea pachetelor de date între rețele de calculatoare. Acesta poate conecta două sau mai multe rețele între ele.

S de la Spear phishing

Salting Proces de prelucrare a parolelor stocate pentru a le spori nivelul de securizare. De obicei, parolele sunt securizate printr-un proces denumit hashing, care atribuie un șir de caractere alfanumerice fiecărei parole. Salting-ul este un proces premergător hashing-ului, prin care parolei îi este atribuit un șir de caractere, pentru a se asigura o valoare diferită a hash-ului. Acest proces asigură o securizare mai bună deoarece parolele identice au hash-ul identic.

Sandboxing Activitate de analiză malware prin care se execută în mod restricționat și controlat un cod într-un server special creat (permite accesarea doar a anumitor resurse software și hardware), cu scopul de a urmări funcționalitățile codului respectiv și de a stabili indicatorii de infectare specifici acelui malware. Se poate folosi și în cazul în care există un cod necunoscut sau care provine din partea unui terț care nu prezintă încredere.

Scam Mod general de a defini diferite tipuri de fraudă cu care se confruntă utilizatorii atunci când folosesc Internetul. Cei care desfășoară astfel de activități folosesc instrumente tehnice sau tehnici de inginerie socială cu intenția de a obține foloase financiare.

Scanare de vulnerabilități Activitate specializată ce vizează căutarea și identificarea vulnerabilităților existente la nivelul unui sistem IT&C.

Scareware (Rogueware) Aplicație malware disimulată ca antivirus pentru a frauda cumpărătorii să o achiziționeze în schimbul unei sume de bani.

Scraping Procesul de colectare și indexare a datelor și informațiilor din diferite surse online, cu ajutorul unui botnet special denumit *scraper*. *Vezi și* Botnet și Crawling.

Script Program scris intr-un limbaj specific (HTML, Java Script, Pearl etc.) care este interpretat și executat de alt program.

Script kiddie (skiddie/script bunny/lamer/noob) Persoană, cu cunoștințe reduse de hacking, care folosește diverse aplicații și script-uri create de hackeri pentru a derula atacuri cibernetice. De regulă, nu deține cunoștințe tehnice și provoca daune din teribilism juvenil, iar pentru a crea iluzia că este hacker, oferă sfaturi pe forumuri într-o manieră arogantă, folosind termeni din jargonul hackerilor.

Search Engine Optimization (SEO) Utilizarea unor strategii, tehnici și tactici de îmbunătățire a vizibilității unor site-uri, atât în scop comercial, cât și pentru susținerea unor activități infracționale în domeniul cibernetic (diseminare de malware, criminalitate informatică etc.).

Secure File Transfer Protocol (SFTP) Protocol ce facilitează accesul, transferul și administrarea fișierelor dintr-un sistem.

Secure Hyper Text Transfer Protocol (SHTTP) Alternativă la HTTPS de securizare a comunicațiilor web.

Secure Hash Algorithm (SHA) Familie de funcții criptografice hash. *Vezi și* Criptare și Hash.

Secure shell (SSH) Protocol ce permite accesul la un sistem IT&C folosind un canal securizat. Securizarea (criptarea) folosită de acest protocol are rolul de a asigura confidențialitatea, disponibilitatea și integritatea datelor transmise printr-o rețea nesigură.

Secure Sockets Layer (SSL) Protocol utilizat pentru criptarea comunicațiilor dintre două puncte din spațiul virtual. Spre exemplu, poate fi utilizat în comunicarea dintre server și browser. Utilizarea acestui protocol este vizibilă prin prefixul *https* din componența URL-ului.

Securitate fizică Măsuri concepute pentru a preveni, detecta și anunța orice tentativă neautorizată de acces la componentele fizice.

Security Information and Event Management (SIEM) Concept utilizat de companiile de securitate cibernetică pentru a defini un produs cu posibilități tehnice ridicate de colectare, agregare, corelare, analiză și raportare în timp real a alertelor de securitate cibernetică generate de aplicații și echipamente hardware.

Security incident responder Persoana care intervine și investighează orice incident de securitate produs asupra unui sistem IT&C sau serviciu.

Semnătură electronică (digitală) Modalitate de verificare a identității unei persoane în mediul virtual.

Server Resursa care găzduiește pagini web și furnizează servicii prin intermediul protocoalelor specifice.

Server Message Block (SMB) Aplicație utilizată pentru a oferi acces comun utilizatorilor unei rețele la resursele acesteia.

Service Set Identifier (SSID) Cod de până la 32 de caractere care este folosit pentru a recunoaște o conexiune de tip WLAN la un router WI-FI și alte puncte de acces. O listă de valori care este vizibilă la căutarea unei conexiuni wireless.

Shell Software care oferă o interfață de acces în care se pot executa diverse comenzi pe un sistem IT&C.

Shellshock (Bashdoor) Vulnerabilități ale sistemului de operare Linux care facilitează accesul, preluarea controlului și indisponibilizarea sistemului țintă.

Sidejacking Atac cibernetic prin care pot fi interceptate comunicațiile electronice ale unui utilizator prin obținerea și folosirea sesiunii unice de autentificare generată de un server pentru acel utilizator.

Single Point of Accountability (SPA/SPOA) Principiul conform căruia toate bunurile și procesele critice să aibă un responsabil desemnat. Raționamentul este bazat pe faptul că în lipsa unor responsabilități clare, delegate unei singure persoane, crește probabilitatea apariției unor vulnerabilități, comparativ cu situația în care mai multe persoane administrează un proces sau o persoană administrează mai multe procese.

Sinkhole O resursă hardware sau software către care poate fi redirectat traficul nelegitim din Internet și care reprezintă totodată un loc în care acesta poate fi analizat.

Smishing Formă de phishing derulată prin intermediul mesajelor SMS. *Vezi și* Phishing.

Sniffing Analiza traficului de date dintr-o rețea sau dispozitiv, monitorizat și înregistrat de un software denumit sniffer, fără a afecta sau modifica datele transmise.

Social media Reprezintă totalitatea platformelor și serviciilor care facilitează conexiunea dintre persoane și comunități cu scopul de a interacționa în mediul online.

Socket Software care acționează ca un punct final de stabilire a unei legături bidirecționale de comunicație între două procese din cadrul aceluiași dispozitiv sau aflate pe dispozitive diferite.

Spam Mesaj electronic nesolicitat.

Spamming Activitatea prin care se distribuie către un număr mare de utilizatori mesaje electronice nesolicitate, într-un interval de timp scurt. De regulă, mesajele au conținut comercial, propagandistic, politic sau pornografic, scopul lor fiind de a indisponibiliza sau infecta infrastructura țintă.

Spoofing Disimularea identității la transmiterea unor mesaje electronice sau la trecerea de filtrele de securitate.

Spațiu cibernetic Mediul virtual, generat de infrastructurile cibernetice, incluzând conținutul informațional procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acesta.

Spear phishing Reprezintă o tehnică asemănătoare cu phishing-ul clasic, diferența constă în faptul că ținta este bine determinată, iar atacul conține elemente personalizate de convingere a potențialelor victime. Metoda este utilizată, de regulă, în cadrul unui atac de tip APT, și constă în transmiterea de mesaje către un grup de utilizatori care au în comun anumite elemente (sunt angajații unei instituții sau companii). E-mailurile sunt concepute astfel încât destinatarul să perceapă expeditorul ca fiind o persoană cunoscută (de la care primește de regulă sau așteaptă corespondență). Atașamentele ce conțin malware (fișiere de tip word, excel, pdf) au denumiri similare domeniului de activitate al destinatarului. *Vezi și* Phishing.

Spionaj cibernetic Acțiune care vizează obținerea accesului neautorizat la informații cu caracter confidențial sau clasificat, stocate în cadrul unui sistem IT&C, cu scopul de a fi utilizate de o entitate străină.

Spyware Software creat pentru sustragerea de date (în special confidențiale, de acces sau bancare) de pe sistemele țintă. Un program de tip spyware nu afectează în mod direct sistemul, dar poate colecta informații pentru un atac ulterior cu o formă diferită de malware. Câteva exemple de aplicații spyware: Flexispy, Arm Spy Software, Phone Sheriff, Mbackup, Spybubble etc.

SQL Injection (SQLi) Vulnerabilitate a unei aplicații, care are atașată o bază de date și care permite unui eventual atacator să altereze interogarea SQL, transmisă bazei de date sau când, prin injectarea sintaxei, logica interogării este modificată astfel încât să execute o acțiune diferită. Exemple de aplicații folosite în atacurile de tip SQL Injection sunt SQLMap și HAVIJ.

Structured Query Language (SQL) Limbaj de programare special conceput pentru gestionarea și manipularea datelor dintr-o bază de date.

Supervisory Control and Data Acquisition System (SCADA) Rețele sau sisteme IT&C folosite pentru comanda și controlul proceselor tehnologice ce au loc în obiective industriale civile sau militare (hidrocentrale, combinate electrice, chimice și petrochimice, centrale atomice etc.). Două exemple de malware utilizat pentru a ataca cibernetic sistemele SCADA sunt Stuxnet și Duqu.

Stegware Metodă de ascundere a codului nelegitim în conținutul unui fișier sau software pentru a fi nedetectabil de soluțiile antivirus.

Surse deschise (Open source) În domeniul cibernetic se referă la scrierea și distribuirea de script, aplicații și software în mediul online pentru a fi utilizate gratuit, modificate sau îmbunătățite.

T de la de la Troian

Tactics, Techniques and Procedures (TTP) Modul în care tehnicile, tacticile și procedurile au fost utilizate în cadrul unui atac cibernetic punctual.

Tampering Acțiune neautorizată care constă în modificarea intenționată a parametrilor sau datelor existente într-un sistem IT&C.

Terorism cibernetic (Cyberterrorism) Activități desfășurate în spațiul cibernetic, de către persoane, grupări sau organizații motivate extremist-terorist (ideologic sau religios), cu scopul de susținere a unor activități de recrutare, radicalizare, propagandă și finanțare *(cyber-enabled-terrorism)*, fie pentru derularea de atacuri cibernetice împotriva unor sisteme IT&C *(cyber-dependent-terrorism)* care pot determina distrugeri materiale sau victime.

Token Dispozitiv electronic (USB, card etc.) utilizat pentru validarea identității și acordarea dreptului de acces la un sistem IT&C, dispozitiv, proces etc..

Tool (Instrument) Instrument utilizat în derularea unui atac cibernetic.

Toolkit (Instrumentar) Set de instrumente utilizat în derularea unui atac cibernetic.

The Onion Router (TOR) Sistem de comunicare ce asigură anonimizarea online.

Transmission Control Protocol (TCP) Set de protocoale utilizat la scară largă, atât în rețelele locale, cât și pe Internet, pentru nivelul de disponibilitate și flexibilitate pe care îl oferă. Dispune de cel mai înalt grad de corecție a erorilor și permite comunicarea dintre calculatoarele din întreaga lume indiferent de sistemul de operare instalat.

Transport Layer Security (TLS) Protocol, bazat pe un algoritm de criptare a datelor, care asigură confidențialitatea pe Internet între aplicațiile folosite pentru comunicare și utilizatorii acestora. În momentul în care un server comunică cu un computer utilizator, TLS asigură inexistența unui terț care să blocheze sau intercepteze comunicația respectivă.

Trivial File Transport Protocol (TFTP) Protocol de transmitere a fișierelor de mici dimensiuni.

Troian Software care aparent are o funcție legitimă și utilă, dar deține și una ascunsă și potențial nelegitimă, care evită mecanismele de securitate, uneori exploatând vulnerabilități ale sistemelor vizate. Astfel, odată instalat, programul poate derula activități nelegitime, precum sustragerea de informații, afectarea calculatorului gazdă sau crearea unor căi disimulate de acces de la distanță la sistemul infectat. *Zeus (Zbot trojan)* este un exemplu de malware de tip troian, apărut în 2007 și îmbunătățit periodic, folosit pentru a extrage informații confidențiale sau sume de bani de la victime. Este folosit în atacuri de tip *phishing* și *driven-by downloads*, iar odată instalat, poate facilita atacuri de tip *keylogging* și/sau *man in the middle.*

Troian bancar Software nelegitim creat pentru a obține acces și extrage date despre conturile utilizatorilor sistemelor bancare online.

Two factor authentication (2FA) *Vezi* Autentificare în doi factori.

UDP flood attack Suprasolicitarea unei aplicații prin trimiterea de comenzi multiple, într-un interval scurt de timp, prin intermediul protocolului UDP, având ca scop obținerea DoS și neutralizarea sistemului firewall. *Vezi și* Denial of Service (DoS) și User Datagram Protocol (UDP).

UDP scan Acțiune de scanare a unui sistem pentru a identifica ce porturi UDP sunt deschise. *Vezi și* Port scan.

Unified Threat Management (UTM) Dispozitiv de securitate care integrează un număr mare de servicii și tehnologii de securitate.

Uniform Resource Identifier (URI) Serie de caractere folosită pentru a identifica un nume sau o resursă web. *Vezi și* Uniform Resource Locator și Uniform Resource Name.

Uniform Resource Locator (URL) Secvență de caractere standardizată folosită pentru denumirea și localizarea unor resurse de pe Internet. Adresa la care poate fi găsită pe Internet o destinație. *Exemplu: Adresa URL a Google este http://www.google.com. Vezi și* Uniform Resource Identifier și Uniform Resource Name.

Uniform Resource Name (URN) Secvență utilizată pentru identificarea și găsirea unor resurse pe Internet, chiar dacă locația acestora este schimbată. *Vezi și* Uniform Resource Locator și Uniform Resource Identifier.

Unitate Centrală de Procesare (UCP) *Vezi* Central Processing Unit (CPU).

Universal Serial Bus (USB) Tip de conexiune standard care se regăsește la majoritate dispozitivelor electronice și permite conectarea altor dispozitive. *Exemplu: Conexiunea dintre tastatură sau memorie externă și calculator.*

Upload Copierea unor fișiere de pe calculatorul clientului pe server.

URL Injection Atac cibernetic asupra unui website prin care sunt create noi pagini web în cadrul acestuia, fără știința administratorului și care pot conține malware sau mesaje spam.

User Behavior Analysis Analiza informațiilor rezultate din activitatea unui utilizator sau a unui grup pentru a înțelege comportamentul și a identifica posibile pattern-uri, cu scopul de a îmbunătăți securitatea cibernetică sau a aplica măsuri de prevenire.

User Datagram Protocol (UDP) Protocol de comunicație unidirecțională între sisteme IT&C, care face posibilă livrarea datelor într-o rețea, fără a verifica disponibilitatea destinației (fără crearea în prealabil a unor conexiuni dedicate între expeditor și destinatar). *Vezi și* UDP flood attack.

User Identity Correlation Validarea activității unui cont sau detectarea accesului neautorizat prin analiza modului în care au fost utilizate drepturile de acces ale utilizatorului.

User Interface (UI) *Vezi* Interfața cu utilizatorul.

Utilizator (User) Persoană sau proces autorizat să acceseze o rețea sau un sistem IT&C.

V de la Virus

Voice over Internet Protocol (VoIP) Protocoale, tehnologii, metodologii de comunicații și tehnici de transmisie angrenate în comunicațiile de voce și sesiuni multimedia prin IP. *Vezi și* Internet Protocol (IP).

Virtual Machine (VM) *Vezi* Mașină virtuală.

Virtual Private Network (VPN) Tehnologie de comunicații, folosită pentru a oferi o conexiune securizată și anonimă între utilizator și domeniile accesate. Conexiunea dintre computerul care trimite datele și computerul care le distribuie la destinatarul real este criptată.

Virtual Private Server (VPS) Serviciu de găzduire web care oferă utilizatorului beneficii similare cu deținerea propriului server, însă la costuri mult mai reduse.

Virus Malware care se poate autoreplica în cadrul unui sistem și propaga în alte calculatoare din rețea fără știința utilizatorului. Se atașează de fișiere și urmărește să se răspândească cât mai eficient. Acesta poate afecta funcționalitatea, integritatea, disponibilitatea sistemului sau datelor stocate. În prezent nu mai este foarte popular printre atacatori.

Vishing (voice phishing) Utilizarea telefonului (chat sau apel) în tentativa de a determina victima să realizeze o acțiune (furnizarea de credențiale sau accesarea unui link infectat) pentru ca atacatorul să obțină acces neautorizat în conturi sau sisteme.

Vulnerabilitate de securitate cibernetică Punct slab al unui software sau sistem IT&C, pe care un atacator îl poate exploata pentru a compromite confidențialitatea, disponibilitatea și/sau integritatea țintei. *Vezi și* Confidentiality, Integrity and Availability (CIA).

Vulnerabilities Equities Process (VEP) Proces de analiză a oportunității de a raporta public sau ține secretă o vulnerabilitate de tip *zero day*.

Watering hole attack (Water-holing) Metodă de atac care constă în compromiterea unui site, despre care există indicii că va fi accesat de către anumite persoane vizate, prin injectarea de script-uri și „așteptarea" victimei de fi infectată.

Web hosting (găzduire web) Serviciu care constă în acordarea unui spațiu pe un server conectat la internet, în vederea publicării unui site web.

Web server Termen ce definește atât componenta hardware (calculatorul), cât și software (aplicațiile), folosite pentru găzduirea conținutului paginilor web (imagini, text, conținut audio-video), accesibile prin intermediul Internetului. Funcția primară a acestuia constă în furnizarea paginilor web, cu ajutorul protocolului HTTP/HTTPS.

Whaling Atac de tip spear phishing care vizează persoane cu un profil ridicat. *Exemplu: persoane din palierul managementului de top din cadrul unor companii internaționale. Vezi și* Spear phishing.

White team Echipa formată din persoane care au rolul de arbitru în cadrul unui concurs de hacking între două echipe, denumite Red Team și Blue Team. *Vezi și* Red Team și Blue Team.

Whitelist Listă de aplicații verificate și cunoscute ca fiind sigure. *Exemplu: Apple App Store.*

Wi-Fi Tehnologia utilizată pentru realizarea comunicației fără fir (wireless) în cadrul rețelelor locale (LAN), la viteze echivalente cu cele ale rețelelor cu fir electric de tip Ethernet.

Wi-Fi Protected Access (WPA) Protocol, bazat pe un algoritm de criptare a datelor, care asigură transmiterea datelor prin intermediul rețelelor wireless, folosit în scopul asigurării confidențialității.

Wide Area Network (WAN) Tip de rețea care facilitează conexiunea la alte rețele pe o zonă geografică extinsă. De obicei, o astfel de rețea este deținută de un ISP. *Vezi și* Internet Service Provider.

Wired Equivalent Privacy (WEP) Protocol, bazat pe un algoritm de criptare, care asigură transmiterea datelor prin intermediul rețelelor wireless.

Wireless Intrusion Prevention System Dispozitiv care poate fi atașat unei rețele pentru a scana spectrul radio în vederea identificării tentativelor de accesare neautorizată prin intermediul tehnologiei wireless.

Wireless Local Area Network (WLAN) Tip de rețea care interconectează dispozitivele dintr-o zonă geografică restrânsă prin intermediul tehnologiei wireless.

World Wide Web (WWW) Sistem format din totalitatea site-urilor și fișierelor multimedia de tip hipertext interconectate care pot fi accesate prin rețeaua de Internet, cu ajutorului unui browser.

Worm (Vierme informatic) Malware care are capacitatea de a se autoreplica și propaga într-o rețea de calculatoare și ulterior în alte rețele, folosind resursele rețelei, fără a se atașa de un program sau proces. Acesta se răspândește prin spațiul de stocare, rețeaua de internet sau USB și devine vizibil doar în momentul în care prezența sa determină încetinirea anumitor aplicații.

X de la XSS

XSS *Vezi* Cross-site scripting.

Y de la Yottabyte

Yottabyte (YB) Cea mai mare unitate de măsură utilizată pentru descrierea capacității de stocare, echivalentă cu 10^{24} bytes sau 10^{15} gigabytes (GB).

Z de la Zero day exploit/vulnerability

Zero day exploit/vulnerability (0 day) Vulnerabilitate a unei aplicații sau a unui sistem, care a fost descoperită de o persoană sau un grup restrâns de persoane, nefiind cunoscută de autorul acesteia și publicul larg, având posibilitatea de a o exploata (în scopuri rău intenționate), comercializa sau raporta.

CENTRUL NATIONAL CYBERINT
2019