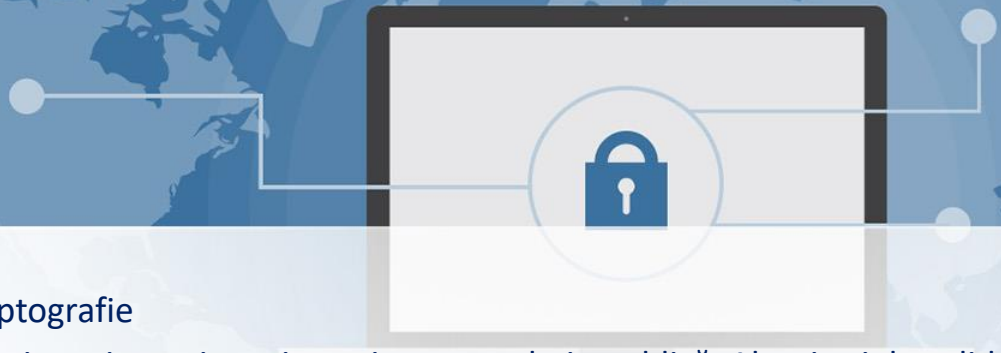
Criptografie și Securitate Cibernetică

RCC – CSC 1

Conținut

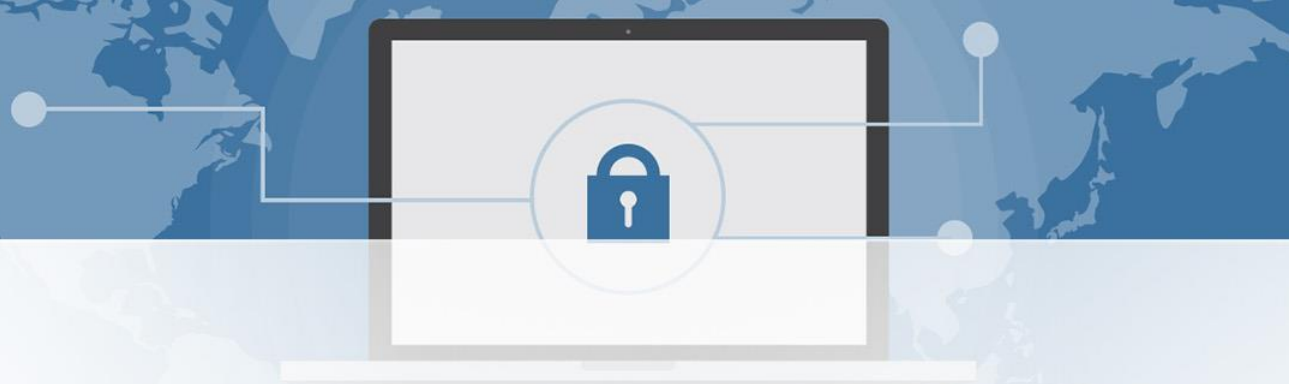


- Noțiuni introductive de criptografie
  - Sisteme criptografice simetrice, asimetrice, criptare cu cheie publică. Algoritmi de validare a datelor
  - Certificate digitale. Semnături digitale
  - Protocoale criptografice de autentificare
  - Securitatea canalelor de comunicații, aplicațiilor și sistemelor informatice
- Elemente de securitatea cibernetică
  - Tipuri de atacuri și amenințări cibernetice. Elemente vulnerabile ale unui sistem informatic
  - Tehnologii pentru asigurarea securității cibernetice. Modalități de prevenție în spațiul virtual
  - Asigurarea securității sistemului la nivel de rețea / la nivelul utilizatorului
  - Securitatea cibernetică a dispozitivelor (desktop, mobile, SO)
  - Managementul incidentelor de securitate cibernetică
  - Investigații de securitate cibernetică – forensics
  - Tehnici și instrumente de evaluare a securității cibernetice a unor sisteme informatice

Bibliografie

1. Adrian Graur, Dimitris Voukalis, Applied Channel Cryptography, Media Mira, 2008
2. Atul Kahate Cryptography and Network Security, McGraw Hill; Third edition, 2013
3. William Stallings, Cryptography and Network Security: Principles and Practice, 6th Edition, 2013
4. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone; Handbook of Applied Cryptography, CRC Press, 2001
5. Wenbo Mao, Modern Cryptography: Theory and Practice, Prentice Hall PTR, 2003
6. Hans Delfs, Helmut Knebl, Introduction to Cryptography, Springer, 2002
7. Oded Goldreich, Foundations of Cryptography, Cambridge University Press, 2004
8. Rolf Oppliger, Contemporary Cryptography, Artech House Publishers, 2005
9. Bruce Schneier, Niels Ferguson, Practical Cryptography, John Wiley & Sons Inc
10. A. Menezes, P. Oorschot, S. Vanstone; Handbook of Applied Cryptography, CRC Press, 2001

Evaluare



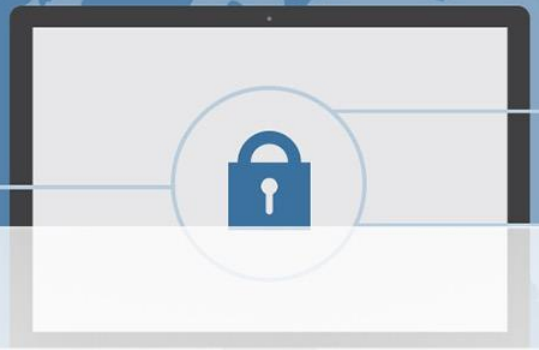
- Nota disciplina = Nota laborator + Nota examen
- Nota laborator = Nota parcurs + Nota Proiect
- Nota examen = Nota parcurs + Nota Referat

Noțiuni introductive de criptografie

- Criptografia
  - origine greacă
    - κρυπτός *kryptós* (ascuns)
    - și γράφειν *gráfein* (a scrie).

  ➢ Metoda matematică
  ➢ Securizarea informației
  ➢ Autentificarea utilizatorilor în sisteme informatice
  ➢ Restricționarea accesului în sisteme informatice

Criptografia Clasică

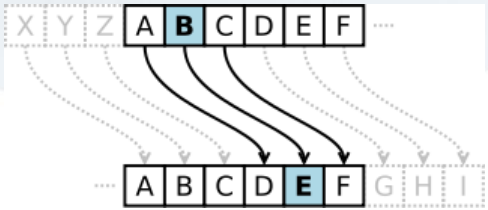


- Termenul **criptografie** face referire la ***criptare***
  - **Criptarea** - conversia informației obișnuite (text în clar) într-un text neinteligibil (*text cifrat*).
  - **Decriptarea** este procesul invers
    (text cifrat --» text în clar)
  - Se bazează pe un **Cifru**
    (algoritmul după care se face atât criptarea cât și decriptarea)
  - Cifrul se bazează pe o **cheie**
    (un element secret, cunoscut doar de cei care comunică informația)

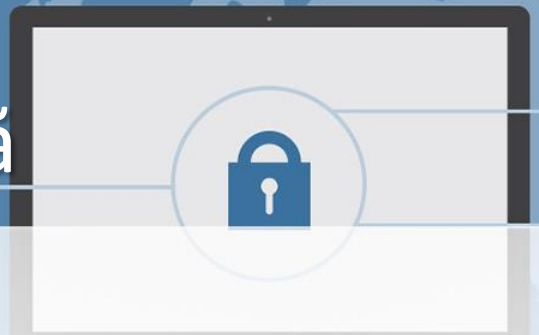
Criptografia Clasică – cifruri

- Principalele tipuri clasice de cifruri
  - ➢ cifrurile cu **transpoziție**
    - ➢ modifică ordinea literelor dintr-un mesaj
      (de exemplu „ajutor” devine „ojartu”)
  - ➢ cifrurile cu **substituție**
    - ➢ înlocuiesc litere sau grupuri de litere cu alte litere și grupuri de litere
      (de exemplu, „conexiune” devine „dpofyjvof” înlocuind fiecare literă cu următoarea din alfabet).

Ex. Cifru lui Cesar
(deplasare de 3)



Criptografia Modernă



- Extinderea criptării (asigurarea confidențialității mesajelor)
  - tehnici de verificare a integrității mesajelor,
  - autentificare a trimițătorului și receptorului,
  - semnătură electronică,
  - calcule securizate...

Criptografia Modernă - CIFRURI

- Criptografia cu chei simetrice
  - trimițătorul cât și receptorul folosesc aceeași cheie
    (mai rar, cheile pot fi diferite)

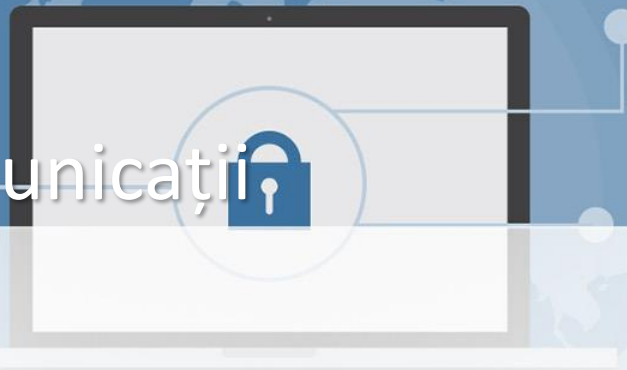
➢ Cifruri pe blocuri
  - la intrare un bloc de text clar și o cheie,
  - la ieșire un bloc de text cifrat de aceeași dimensiune

❖ Cifruri standard
  - ❖ Data Encryption Standard (DES)
  - ❖ Advanced Encryption Standard (AES)

➢ Cifruri pe flux
  - creează dinamic o cheie arbitrară, care este combinată cu textul clar, bit cu bit sau caracter cu caracter

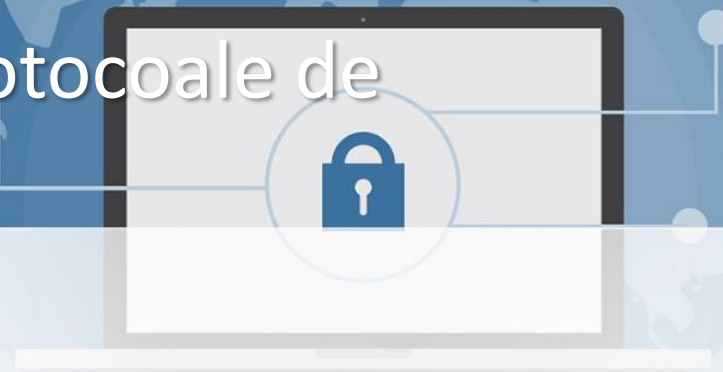
❖ Ex. RC4

Criptografia Canalelor de comunicații



- Elemente de bază
  - Modelul de securitate OSI
    (cadrul de definire a securității informatice)
    - Protocoale, Mecanisme, Servicii
  - Atacuri informatice de securitate
    - Citirea neautorizată de mesajelor (fișiere sau trafic de date)
    - Atacuri active
      - (modificarea de mesaje sau trafic)
      - sau DoS (Denial of Service)
  - Mecanisme de securitate
    - Detecția, prevenirea și refacerea după un atac informatic
  - Servicii de securitate
    - Autentificare, controlul accesului, confidențialitatea datelor, integritatea datelor, respingerea conexiunilor, disponibilitatea serviciilor

Algoritmi și protocoale de criptare

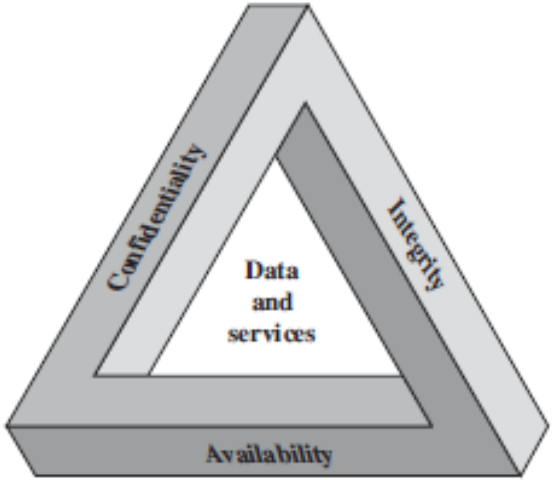


- Categorii
  - Criptare simetrică
    - Ascunderea conținutului pe blocuri sau fluxuri de date datelor de orice dimensiune (mesaje, fișiere, parole)
  - Criptare asimetrică
    - Criptarea blocurilor de date de dimensiuni reduse (chei de criptare sau hash-uri din semnăturile digitale)
  - Algoritmi de verificare a integrității datelor
    - Protejarea la modificare a blocurilor de date
  - Protocoale de autentificare
    - Autentificarea identității utilizatorilor, pe baza unui algoritm criptografic

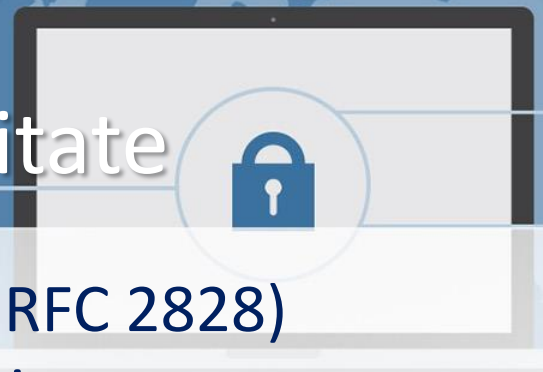
Securitatea comunicațiilor în rețea

- Vizează măsuri pentru
  - Oprirea,
  - Prevenirea,
  - Detecția,
  - Corectarea
    încălcării regulilor de securitate.

- Securitatea comunicațiilor
  - Confidențialitatea
    - Date private, intimitate utilizator
  - Integritatea datelor
    - Date, sisteme complete, nemodificate
  - Disponibilitatea
    - Servicii accesibile, accesul utilizatorilor



Evenimente de securitate

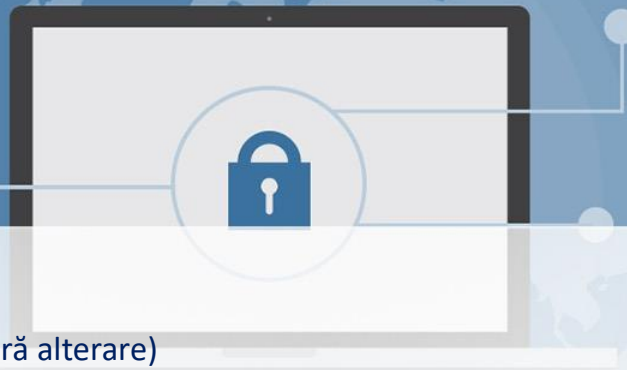


- Evenimente de securitate (RFC 2828)
  - ➢Vulnerabilitatea de securitate
    - o posibilă breșă de securitate care există și poate fi exploatată în anumite circumstanțe,
    - care poate afecta sistemul informatic, dacă este utilizată
  - ➢Atacul informatic
    - atacul intenționat asupra unui sistem informatic,
    - evitarea serviciilor de securitate,
    - Încălcarea regulilor de securitate

Modelul de securitate OSI

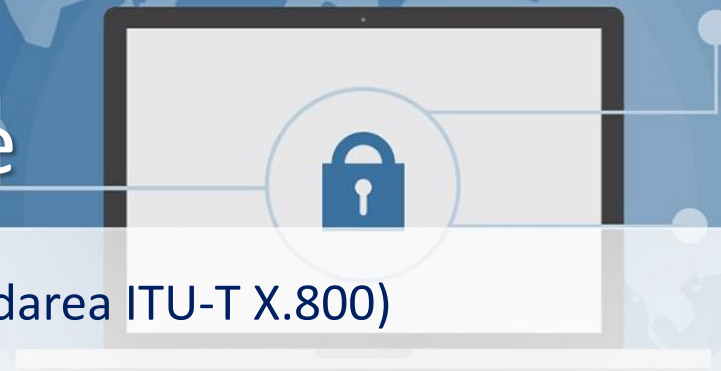
- Concepte de bază ale modelului de securitate
- OSI (Open Systems Interconnection)
  - Atacul informatic
    - Acțiune ce compromite sistemul de securitate al unei organizații
  - Mecanismul de securitate
    - Un proces (dispozitiv) creat pentru a detecta sau preveni atacurile și de a recupera sistemul informatic după atacuri.
  - Serviciul de securitate
    - Un serviciu de comunicație care se folosește de un mecanism de securitate pentru a permite un anumit nivel de securitate a procesării și transferului datelor

Atacuri informatice



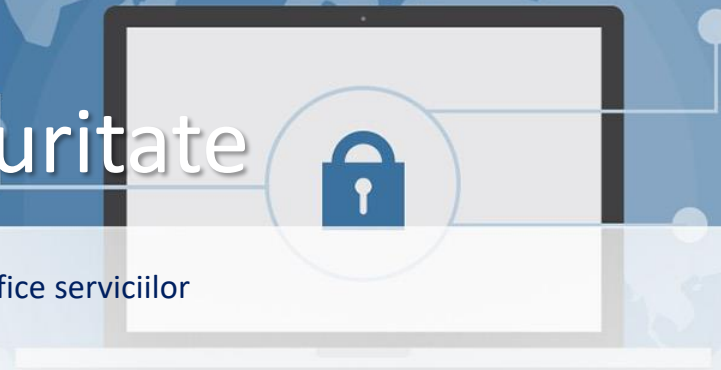
- Atacuri pasive
  - Obținerea informațiilor transmise (fără alterare)
  - Interceptarea traficului
  - Monitorizarea traficului
- Atacuri active
  - Modificarea datelor transmise (sau date false)
  - Mascarea datelor
    - O entitate pretinde că are o altă identitate
  - Retransmitere
    - Capturarea și retransmiterea datelor modificate
  - Modificarea mesajelor
    - Modificarea parțială a unui mesaj
  - DoS (Denial of Service)
    - Reduce sau suprimă utilizarea normală a unui sistem

Servicii informatice



- Servicii informatice (Recomandarea ITU-T X.800)
  - Autenticitatea
    - Asigură faptul ca discută cu punct de rețea autentic
  - Controlul accesului
    - Prevenirea utilizării neautorizate a resurselor
  - Confidențialitatea datelor
    - Protejarea datelor față de divulgarea neautorizată
  - Integritatea datelor
    - Se asigură că datele primite sunt identice cu cele trimise
  - Asigurarea conexiunilor
    - Oferă protecție împotriva respingerii conexiunilor

Mecanisme de securitate



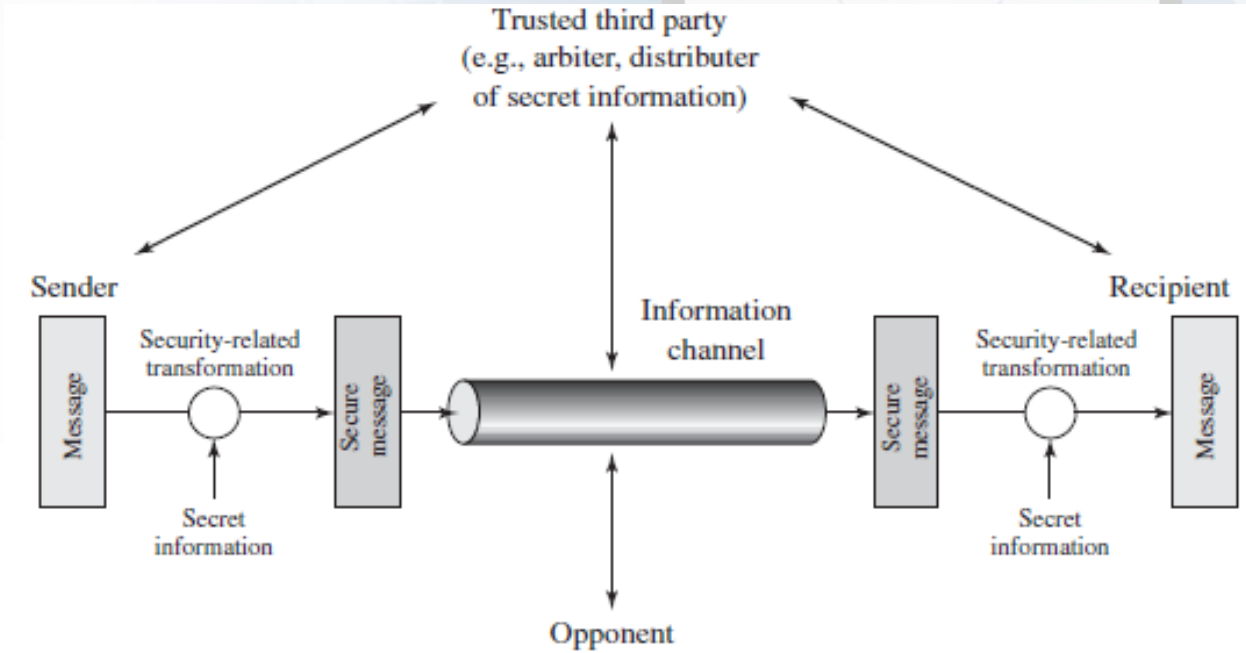
- Mecanisme de securitate specifice serviciilor
  - Cifru criptografic
  - Semnătura digitală
  - Controlul accesului
  - Integritatea datelor
  - Mesaje de autentificare
  - Surplus de trafic
  - Controlul dirijării pachetelor
  - Autentificarea entităților
- Mecanisme omniprezente
  - Funcționalitate
  - Nivel de securitate
  - Detecția evenimentelor de securitate
  - Audit de securitate
  - Refacerea nivelurilor de securitate

Relația dintre servicii și Mecanisme

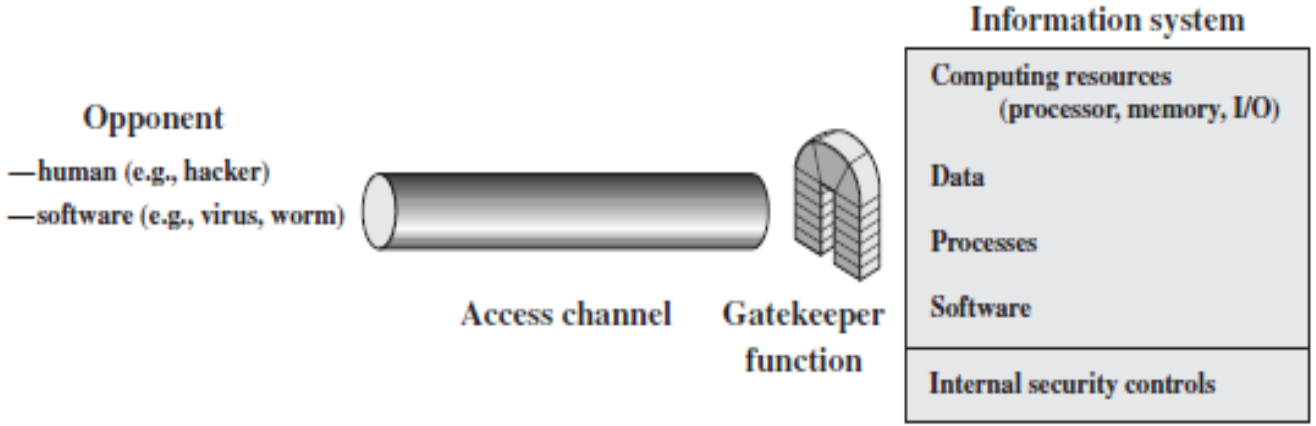
Mechanism

Service	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Peer Entity Authentication	Y	Y			Y			
Data Origin Authentication	Y	Y						
Access Control			Y					
Confidentiality	Y						Y	
Traffic Flow Confidentiality	Y					Y	Y	
Data Integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Model de securitate de rețea



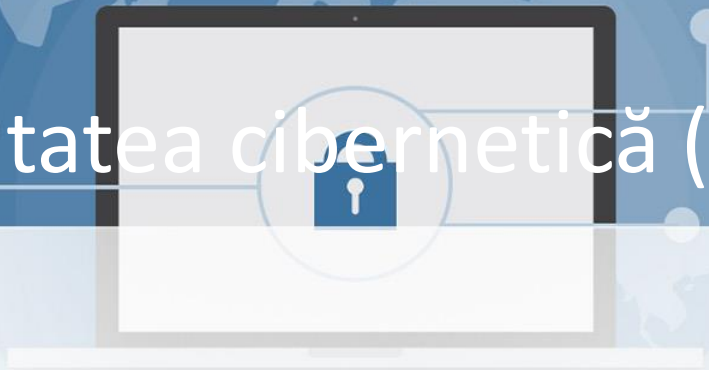
Model de acces la rețea securizat



Elemente de securitate cibernetică

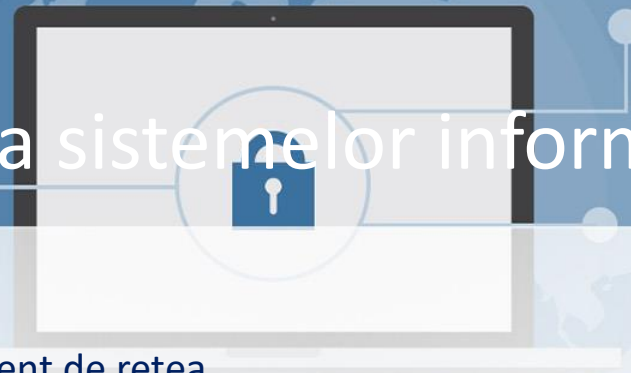
- Fundamentele securității cibernetice
  - Concepte de bază
  - Principiul Least Privillege
  - Principiul CIA (Confidentiality Integrity Availability)
  - Metode de autentificare
- Securitatea rețelelor
  - Stiva TCP/IP
  - Protocolul TCP, UDP
  - Serviciul DNS
  - Translatare -NAT
  - Echipamente de rețea

Elemente de securitatea cibernetică (2)



- Tipuri de atacuri
  - Malware
  - Phising
  - Web Application Attacks
  - Dos și DD0S
  - Man In — The — Middle
- Tehnologii pentru asigurarea securității cibernetice
  - Antivirus
  - IPS/IDS
  - VPN
  - Firewall

Securitatea cibernetică a sistemelor informatice



- Definiția unui sistem informatic
  - Funcționalități: client, server, echipament de rețea
  - Plasarea în cadrul unei rețele
- Explicarea zonelor vulnerabile ale unui sistem informatic
  - Zona de atac la nivel de rețea
  - Zona de atac la nivel de aplicație (aplicații instalate ce interacționează cu utilizatorul, sistemul de operare)
- Asigurarea securității sistemului informatic la nivel de aplicație
  - Vulnerabilități ce se regăsesc la nivelul aplicațiilor: buffer overflow, use after free
  - Metode implementate la nivelul sistemelor de operare pentru a preveni exploatarea
  - Aplicații pentru asigurarea securității sistemelor informatice: antivirus, firewall, HIPS, HIDS

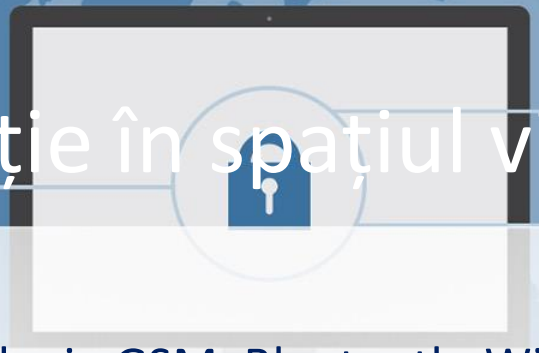
Securitatea cibernetică a sistemelor informatice (2)

- Asigurarea securității sistemului la nivel de rețea
  - Implementarea unui firewall
  - Asigurarea accesului la distanță pentru sisteme informatice (Remote Desktop, VPN, SSH, etc.)
- Modalități de autentificare la nivel de rețea: politici pentru credențiale, modalități de autentificare în doi pași
  - Implementarea unui sistem IDS/IPS (Snort, Suricata, etc.)
- Asigurarea securității sistemelor informatice la nivelul utilizatorului
  - Campanii de conștientizare
  - Instruirea utilizatorului referitor la tehnici de inginerie socială: phishing, mesaje de email cu documente ce conțin diverse modalități de infecție (macrouri, vulnerabilități)
  - Instruirea utilizatorului privind bune practici: asigurarea actualizărilor aplicațiilor și a sistemului de operare, credențiale.

Securitatea cibernetică a dispozitivelor (mobile)

- Tipuri de sisteme de operare pentru dispozitivele mobile
  - Android iOS Windows
- Vulnerabilități ale sistemelor de operare mobile
  - Rooting/ Jailbreak. Tipuri de malware. Vulnerabilități wireless/bluetooth/NFC/GPS. Vulnerabilitățile datelor din cloud.
- Metode de securizare ale dispozitivelor mobile
  - Elemente de securitate oferite de sistemele de operare. Criptarea. Antiviruși.
- Instrumente pentru analiza dispozitivelor mobile
  - ADB. Emulatoare. Android Studio. Reversing APK.
- Elemente de investigare ale dispozitivelor mobile
  - Tipuri de extracții de date. Analiza bazelor de date. Recuperarea datelor șterse.

Modalități de prevenție în spațiul virtual

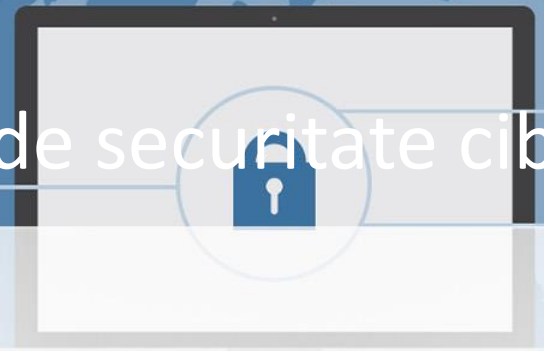


- Conceptul de ”spațiu virtual”
  - Echipamente dotate cu tehnologie GSM, Bluetooth, WiFi sau NFC. De la carduri bancare, ia mașini de spălat și automobile. Web, deep web, dark web. Site-uri, forumuri, aplicații. Internet of Things - IoT, IoE.
- Elemente constitutive ale identității în spațiul virtual
  - Hardware și software. Profiluri și identități fictive. Furtul de identitate. Stereotipuri și pattern-uri comportamentale.
- Anonimizarea — iluzia anonimatului
  - Virtual Private Network. Aplicații dedicate anonimizării. Internet browsere și Sisteme de operare. Anonimizare hardware.

Modalități de prevenție în spațiul virtual (2)

- Elemente de interes legate de prezența în spațiul virtual
  - Stabilirea identității, a preocupărilor și a cercului relațional. Atacuri informatice legate de operațiuni bancare, botnet, mining, ransomware. Clasificarea tipurilor de interese. Interese economice, militare, ne/legale.
- Prevenția în spațiul virtual — o măsură activă, permanentă, continuă și susținută
  - Vulnerabilități și vulnerabilizări. Politici de securitate: de la proiectare, la utilizare. Auditul de securitate white hacking.
- Legislație
  - Legislație națională și internațională. Modalități de intervenție. Autorități competente.

Gestiunea incidentelor de securitate cibernetică

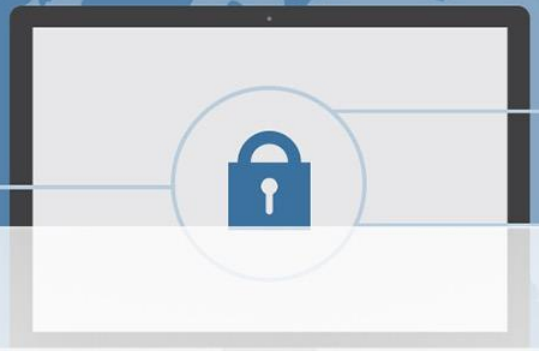


- Introducere în Cyber Defense
  - Descriere Kill Chain (etapele unui atac). Atacuri tradiționale vs. atacuri moderne. Vectori de risc.
- Arhitectura de securitate a infrastructurilor cibernetice
  - Tehnologii de securitate și roluri în securizare (Router, Switch, Firewall, WAF, NIDS/NIPS, UTM/NGFW, Sandbox, Proxy, SIEM/SOC, Packet capture, Honeypot, Threat intelligence
- Arhitectura și principiile ce stau la baza unui SIEM/SOC
  - *Security Information and Event Management / Security Operations Centre*
  - Analiza serviciilor importante de rețea. Analiza avansată la nivelul stațiilor de lucru (endpoint). Managementul incidentelor de securitate

Analiză malware

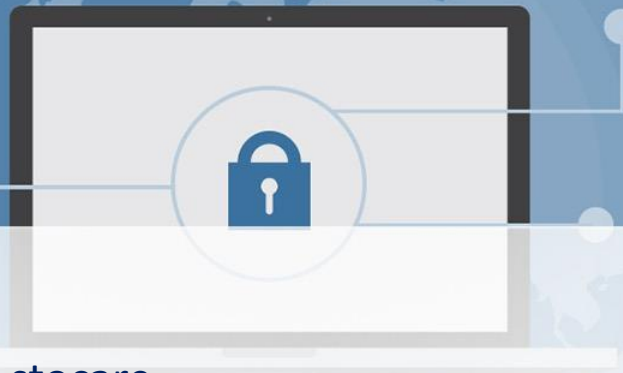
- Noțiuni introductive
  - Definiții și istoric aplicații malware. Tipuri de fișiere și modalități de rulare (fișiere executabile, scripturi, fișiere web, compilatoare, interpretoare, stagii intermediare). Clasificare malware. Tehnici de propagare ale aplicațiilor malware. Vectori de atac și risc. Incident response. Analiză malware și Reverse engineering. Dezasamblare și Decompilare. Antivirus. Importanța unui timeline al evenimentelor în cazul unui incident.
- Tehnici de analiză malware
  - Instalare laborator de analiză malware și sandbox. Sisteme de operare. Sisteme de fișiere. Arhitectura calculatoarelor. Limbajul de asamblare. Structura PE (Portable Executable). Windows API. Aplicații utilizate în procesul de analiză malware. Analiza caracteristicilor statice. Analiză comportamentală. Sandbox și Honeypot. Analiză statică și dinamică avansate (analiza codului și debugging)
- Inginerie inversă — Aplicații executabile
  - Concepte de bază. Funcții de asamblare. Control Flow. API Patterns în malware. Stack. Metode de protecție (packing, ascundere, metode anti-reverse, etc.) 64 bit code

Analiză malware (2)



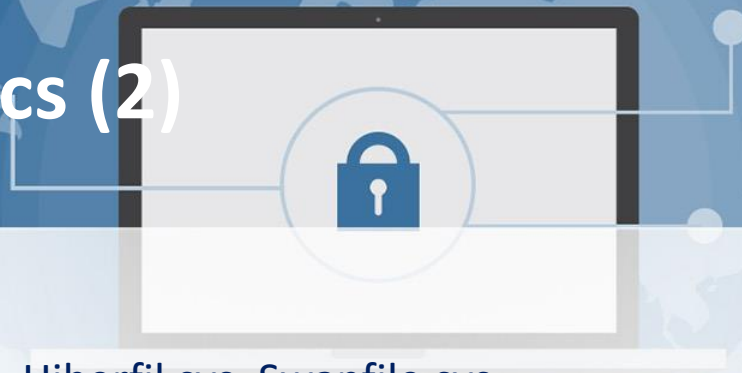
- Analiză scripturi, documente și fișiere web
  - Analiză fișiere web (php, javascript). Analiză log-uri web.. Analiză documente PDF, Office, RTF malițioase.
- Analiză memorie.
  - Înțelegerea modului de funcționare al memoriei. Dump de fișiere din memorie. Analiză memorie (achiziție, analiză). Debug pentru executabile protejate de packere. Injectare cod și API Hooking.
- Analiză Trafic
  - Research adrese de domeniu, adrese IP. Malware networking (topologii, DGA, tunneling). Snort, Wireshark
- Automatizare și hunting
  - Surse online de hunting. Automatizare. Indicatori de compromitere (IoCs). Reguli YARA, yarGen și Loki

Investigații - forensics



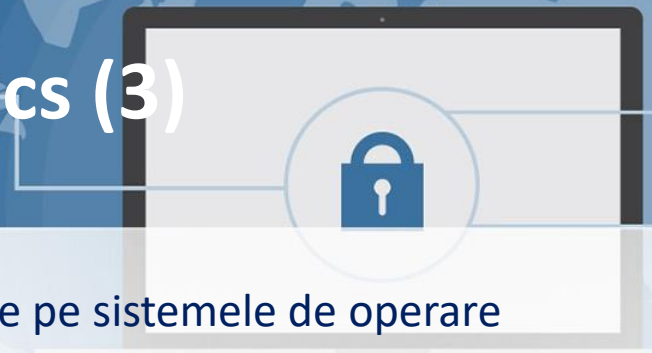
- Introducere IT Forensics
- Achiziția datelor de pe dispozitivele de stocare
  - Hardware (LogicCube, Tableau, etc.)
  - Software (FTK Imager, Encase, DD, Paladin, LiveB00t)
  - Prin rețea (F-Response, Netcat, GRR)
- Tehnici instrumente folosite pentru achiziția memoriei RAM de pe toate sistemele de operare
  - Windows (Magnet, FTK Imager, Memdump, DumplT).
  - Linux (LiME Linux Memory Extractor)

Investigații – forensics (2)



- Analiza memoriei RAM
  - Analiza fișierelor Pagefile.sys, Hiberfil.sys, Swapfile.sys.
  - Extragerea fișierelor shimcache prefatch.
  - Extragerea artefactelor utilizând Volatility, Rekall, Redline. Analiza conexiunilor efectuate de sistemul de calcul (connscan, sockets, connections, netscan).
  - Analiza proceselor extrase din memoria RAM (Pslist, Pstree, Psscan, memdump).
  - Analiza codului injectat in memoria RAM (malfind, Idrmodules).
  - Extragerea informatiilor de interes din regiștri prin intermediul plugin-urilor (Hivelist, Hivedump, Printkey, Userassist, Hashdump).
  - Automatizarea procesului de analiză a memoriei RAM (MemGator Voldiff)

Investigații – forensics (3)

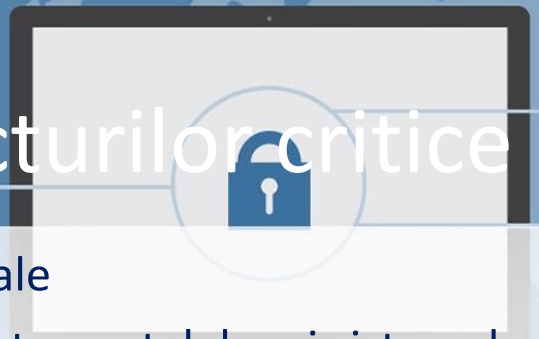


- Analiza fișierelor de jurnalizare de pe sistemele de operare
  - Windows Event Logs (i. System / ii. Application / iii. Security Event Logs).
  - Linux Logs (i.OS Logs (messages.log, daemon.log, dmsg, security, cron, kern.log) ii. Apache Logs (acces.log, error.log) iii. Autentificare (auth.log, wtmp.log, lastlog.log, btmp) iv. Mysql Database (mysqld.log))
- Analiza elementelor de tip forensics de pe sistemele de operare
  - Analiza: regiștrilor, utilizatorilor, conexiunilor la retea, dispozitivelor USB, evenimentelor in timp (timeline), volum shadow copy
- Tehnici de identificare a metodelor antiforensics
  - Sistemul de fișiere. Anomalii ale fișierului timeline, Fișiere șterse, chei de regiștri, Timestamp alterat

Tipuri de amenințări cibernetice

- Troieni/ Viermi
- Injecție de cod (SQLi, XSS)
- Kit-uri de exploatare (Adobe Reader, Flash, JRE, etc.)
- Botnet/Apt
- Denial of Service (Dos, DDos)
- Phishing
- Compromiterea informațiilor confidențiale (încălcare a securității datelor)
- Rogueware/scareware (softuri 'false' de securitate, ransomware)
- Spam
- Atacuri direcționate (inginerie socială)
- Furt/Pierderi/Distrugere fizică device
- Furt de identitate
- Scurgere de informații (targeted attacks)
- Manipularea motoarelor de căutare (includere de link-uri sponsorizate cu referințe spre site-uri malițioase, Xss)
- Certificate digitale false ('man in the middle', vulnerabilități PKI)
- Drive-by exploits (Java by Drive, etc.)

Securitatea infrastructurilor critice

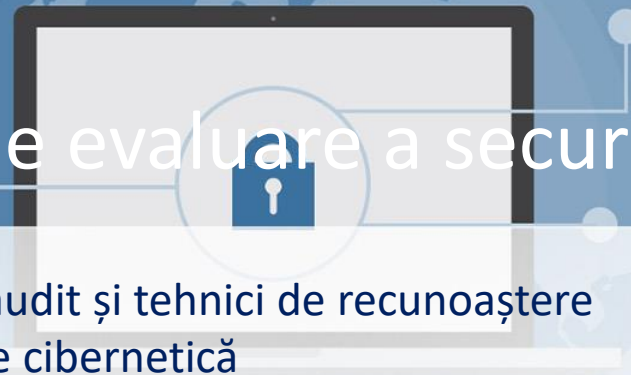


- Infrastructuri critice și servicii esențiale
- Implementarea măsurilor de securitate a rețelelor și sistemelor informatice
  - Managementul drepturilor de acces. Conștientizarea și instruirea utilizatorilor. Jurnalizarea și asigurarea trasabilității activităților. Testarea și evaluarea securității rețelelor și sistemelor. Managementul configurațiilor. Asigurarea disponibilității și funcționării serviciului. Managementul identificării și autentificării utilizatorilor. Răspunsul la incidente
  - Mentenanța rețelelor și sistemelor informatice. Managementul suporturilor de memorie externă. Protecția fizică a rețelelor și sistemelor.
  - Planurile de securitate. Securitatea personalului. Analizarea și evaluarea riscurilor. Protecția produselor și serviciilor aferente rețelelor și sistemelor informatice. Managementul vulnerabilităților și alertelor de securitate

Securitatea infrastructurilor critice (2)

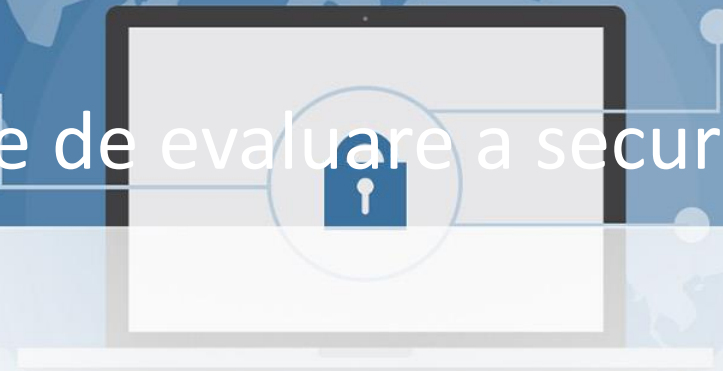
- Securitatea rețelelor informatice industriale
  - sistem de control industrial
- Protocoalele de control industrial
  - Modbus, ICCP/TASE2, DNP3, OLE
  - Alte protocoale utilizate (Ethernet/1P, Profibus, EtherCAT, SERCOS etc.)
- Funcționare sistemelor de control industrial
  - Principalele tipuri de componente: IED, RTU, PLC, HMI, supervisory workstations, data historians etc. Arhitecturi de rețea. Control System Operations. Control Process Management. Smart Grid Operations
- Vulnerabilități și evaluarea riscului
  - Separarea componentelor de rețea și monitorizarea acestora. Excepții, anomalii și detectarea amenințării

Tehnici și instrumente de evaluare a securității



- Planificarea, definirea domeniului de audit și tehnici de recunoaștere
  - Principii ale auditului de securitate cibernetică
  - Tipuri de audit de securitate
  - Metodologia procesului de audit și reguli de angajare
  - Definirea domeniului de testare
  - Procesul de recunoaștere
  - Extragere informații folosind motoare de căutare Raportare
- Scanare și culegere de informații
  - Scopul culegerilor de informații și tipuri de scanări
  - Scanare de porturi
  - Identificare sisteme de operare și servicii active
  - Identificare vulnerabilități Web și de Rețea

Tehnici și instrumente de evaluare a securității (2)



- Exploatare
  - Categorii de exploit-uri
  - Exploatarea vulnerabilităților Web
  - Exploatarea vulnerabilități Rețea
  - Activități Post Exploatare
- Post- Exploatare și Pivotare
  - Colectare de fișiere și informații de pe terminalele compromise
  - Powershell și Bash pentru pentesting
  - Atacuri asupra parolelor: definiții și metodologii. Tipuri de parole și hash-uri