

Retele de calculatoare

Introducere in securitate

Lenuta Alboaie
adria@info.uaic.ro

Cuprins

- Preliminarii
- Aspecte importante
- Vulnerabilitati
- Atacuri
- Prevenirea si supravietuirea
- Monitorizarea
- Testarea
- Raspunsul la incidente
- Protocoale
- Probleme specifice
- Statistici 2015
- Previziuni 2016

*Multumiri:

Sabin Corneliu Buraga
Dragos Acostachioaie

Preliminarii

- Asigurarea calitatii aplicatiilor (Internet)
 - Corectitudine si robustete (*reliability*)
 - Extindere & reutilizare (*modularitate*)
 - Compatibilitate
 - Eficienta
 - Portabilitate
 - Usurinta in utilizare (*usability*)
 - Functionalitate
 - Relevanta momentului lansarii (*timeliness*)
 - Mentenabilitate
 - Reparabilitate, economie
 - **Securitate**

Preliminarii

- **Incident de securitate** = eveniment aparut in cadrul retelei, cu implicatii asupra securitatii unui calculator sau a retelei
 - Sursa: interiorul ori exteriorul retelei
- **Securitatea este procesul de mentinere a unui nivel acceptabil de risc perceptibil**
 - “*Security is a process, not an end state.*” (Mitch Kabay, 1998)
- **Cracker versus hacker**
- **Realitatea:**
 - Peste 70% din organizatii sufera de pierderi financiare datorate incidentelor de securitate
 - Cauze:
 - Virusi informatici: > 75%, Acte malitioase interne: > 40%, Actiuni malitioase externe: 25%, Erori software: 70%, Spionaj industrial: 10%

Preliminarii

- **Mituri:**

- Securitatea prin obscuritate (*security through obscurity - STO*)
 - “*bunk mentality*” security
 - Ignorarea problemelor
 - Nedocumentarea erorilor cunoscute, algoritmilor de criptare folositi
- Cracker-ii “*ascunsi*” nu pot fi detectati
- Organizarea in grupuri malefice a *crackeri*-lor
 - Deseori nu (exceptii: Cult of Dead Cow, ...)
- Software-ul de scanare de virusi ofera protectie totala
- Conexiunile internet nu pot fi detectate
- Din moment ce un fisier este sters, el se pierde pentru totdeauna

Preliminarii

- Faze ale procesului de securizare:

security audit

- Estimare a riscurilor (*assessment*)

- Activitati manageriale +
actiuni tehnice

- Protejare (*protection*)

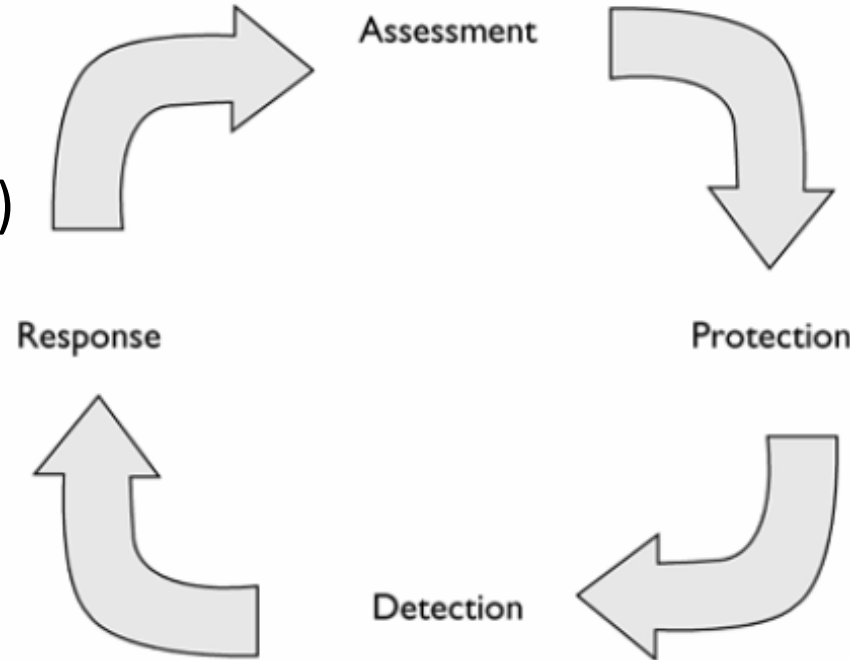
- Prevenire

- Detectare (*detection*)

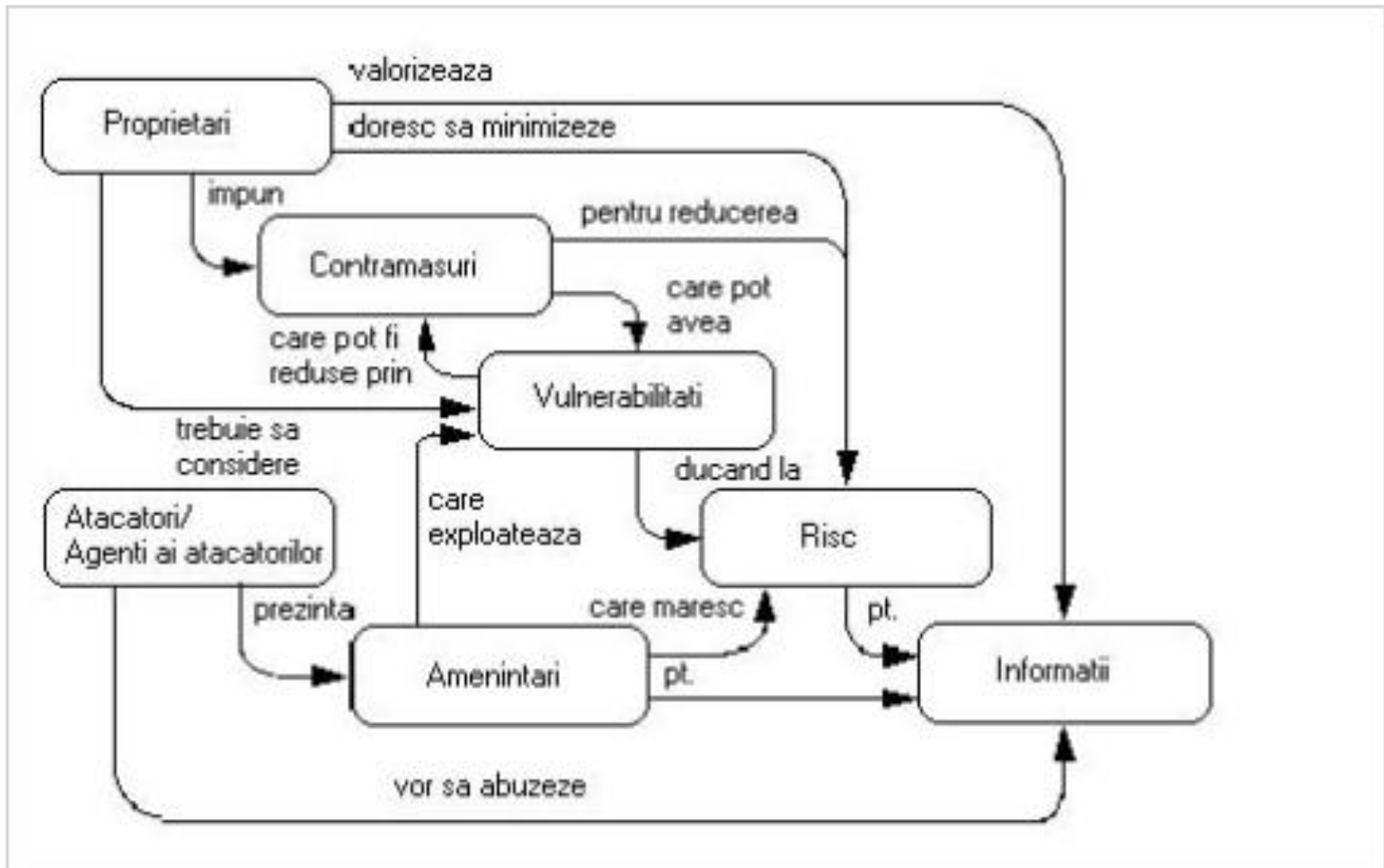
- Identificarea incidentelor (intrusions)

- Raspuns la atacuri (*response*)

- Restaurarea functionalitatii (*patch & proceed*)
- Alegerea remediilor legale (*pursue & prosecute*)



Preliminarii




<http://www.securitatea-informatica.ro/securitatea-informatica/riscurile-de-atac-asupra-securitatii-sistemelor-informationale/>

Forme de protectie

- Controlul accesului
 - Identificarea
 - Autentificarea
 - Autorizarea
 - Acces
- Confidentialitatea
- Intimitatea (*privacy*)
- Integritatea
- Disponibilitatea
- Nerepudierea

Forme de protectie

- **Controlul accesului**

- Proces prin care se ofera sau nu acces la resursa/serviciu
- Terminologie
 - Identificare
 - Exemplu: introducerea *username*
 - Autentificare – “**verify that someone is who they claim they are**”
 - Exemplu: introducerea parolei
 - Serverul ofera suport pentru autentificari de baza sau bazata pe algoritmi de tip *digest* (e.g. MD5)
 - Ex. mecanisme dedicate: Kerberos, RADIUS, TACACS+,...
 - Autorizare
 -  Eavesdropping [RFC1510](http://www.rfc1510.com/).
 - “**determines what a user is and is not allowed to do**”
 - Specifica actiunile (rolurile) pe care un utilizator le poate realiza
 - Exemplu: utilizatorul autorizat are dreptul sa fie logat?
 - Acces
 - Politici care definesc efectiv permisiuni sau privilegii
 - Exemplu: accesul utilizatorului la anumite date (intr-un interval orar sau doar de la un anumit IP, setari facebook – cine poate vedea o resursa?)

Forme de protectie

Controlul accesului - Modele

- Mandatory Access Control (MAC)
 - *End-user*-ul nu poate modifica/transfera controlul asupra resurselor
- Discretionary Access Control (DAC)
 - Detinatorul resursei poate acorda drepturi acesteia si altor utilizatori
 - Ex. Apple Macintosh, UNIX, Windows (User Account Control (UAC)) cer aceasta permisiune cand un soft este instalat
- Role Based Access Control (RoBAC)
 - Asigneaza permisiuni unui rol in organizatie, apoi unui utilizator i se asociaza acest rol
- Rule Based Access Control (RuBAC)
 - Asigneaza controlul in mod dinamic unui utilizator pe baza unui set de reguli. Fiecare resursa contine un set de proprietati de acces bazate pe aceste reguli.
 - Exemplu: Cineva din reseaua A doreste sa acceseze o resursa din reseaua B; RBAC include regula ca daca cineva are adresa din reseaua A poate accesa resursele din B;

Forme de protectie

- **Controlul accesului** – Implementari
 - Sisteme de control - la nivel hardware
 - Accesul la terminal (e.g. verificarea amprentelor, senzori *real-time anti-break*)
 - Visual event monitoring
 - Carduri de identificare
 - Identificare biometrica (e.g. recunoastere - fingerprint, iris & voice recognition)
 - Sisteme de control - la nivel software
 - Drepturi de acces (permisiuni) + liste de control al accesului (ACL – *Access Control List*)
 - Tehnici de tip SSO (*Single Sign-On*)

Forme de protectie

- **Confidentialitatea**

- Imposibilitatea unei terte entitati sa aiba acces la datele vehiculate intre doi receptori
- Solutii:
 - Conexiuni private intre cele 2 puncte terminale ale canalului de comunicatie; datele circula printr-un tunel oferit de o retea privata virtuala (VPN – *Virtual Private Network*)
 - Criptarea datelor via diverse tehnici (biblioteci specializate si/sau oferite de mediile de dezvoltare)
 - Emitatorul cripteaza mesajele
 - Receptorul decripteaza mesajele

Forme de protectie

- **Intimitatea** (*privacy*)
 - Confundata, deseori cu confidentialitatea care se aplica datelor
 - Vizeaza drepturile ce trebuie respectate privind caracterul datelor vehiculate
 - Brese:
 - Stocarea necorespunzatoare a datelor la nivel de server (*information disclosure*)
 - Atacuri de tip *phishing*
 - Configurarea necorespunzatoare a sistemelor

Forme de protectie

- **Integritatea**

- Implica detectarea incercarilor de modificare neautorizata a datelor transmise
- Solutii:
 - Algoritmi de tip *digest*
 - Semnaturi digitale


- **Disponibilitatea**

- O anumita resursa poate fi accesata la momentul oportun
- Cauze ale indisponibilitatii
 - Atacuri de refuz al serviciilor DoS (*Denial Of Service*),
Atacuri distribuite de tip DDoS (*Distributed DoS*) – (vezi slide 22)

Forme de protectie

- **Nerepudierea**

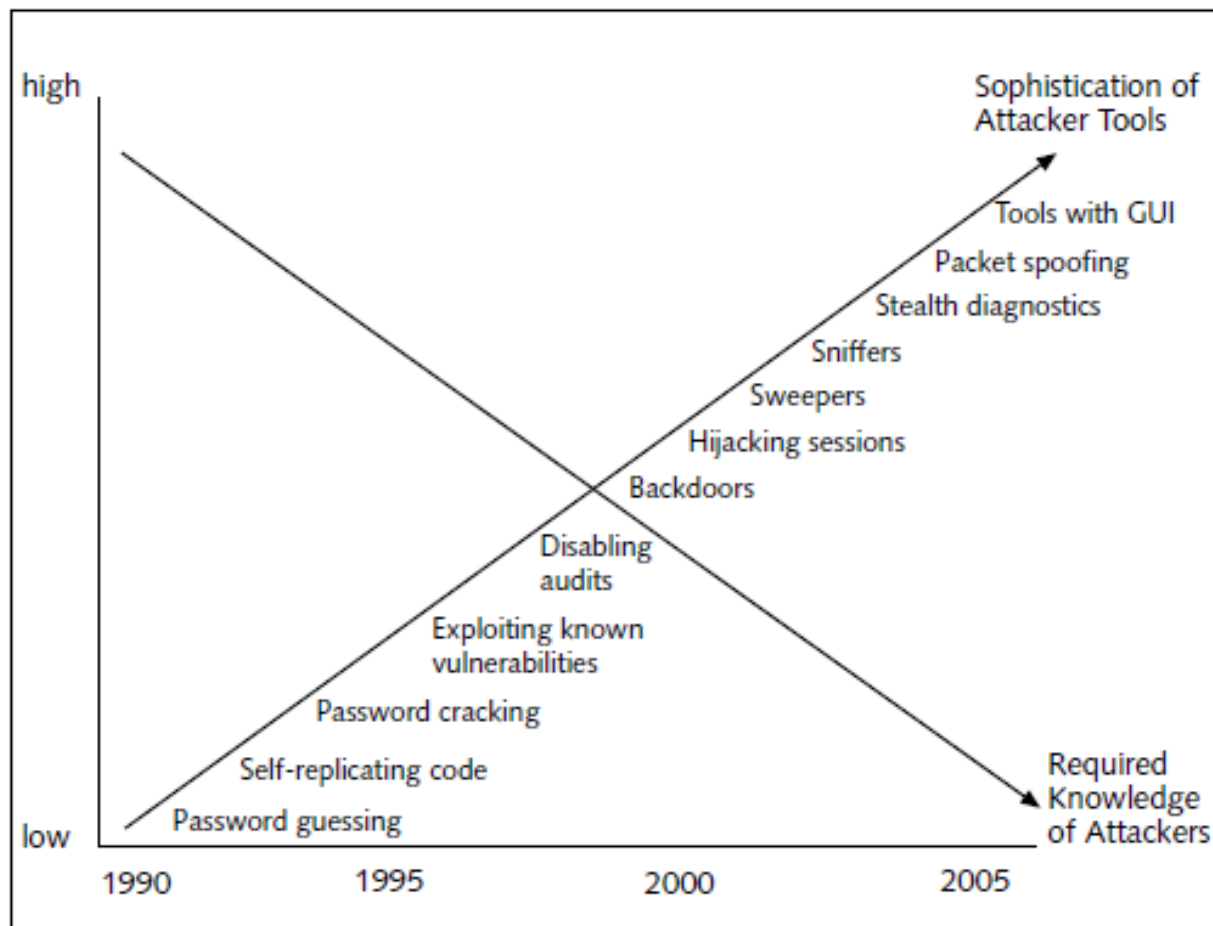
- Expeditorul mesajului nu poate afirma ca nu l-a trimis
- Solutie: certificate digitale
 - Stocheaza datele privind identitatea unei entitati detinatoare a unui secret (parola, serie a cartii de credit, certif. digital, ...)
 - Emise de o autoritate de certificare (CA – *Certification Authority*)
 - Verificate de o autoritate de inregistrare (RA – *Registration Authority*)
 - Serviciile PKI puse la dispozitie de sistem



Infrastructura
cu chei publice
(PKI - *Public*
Key
Infrastructure)

Dificultati in apararea contra unui atac

- Viteza de atac
 - “Slammer worm infected 75,000 computers in the first 11 minutes after it was released and the number of infections doubled every 8.5 seconds”
- Complexitatea atacului
- Disponibilitatea instrumentelor de atac
- Detectarea rapida a vulnerabilitatilor
- *Delay patching*
- Atacuri distribuite
- Confuzia utilizatorilor



[Security guide to network security fundamentals, Mark Ciampa]

Vulnerabilitati

- Pentru Internet, securitatea trebuie sa ia in considerare:
 - Clientul: interactiune, date personale,...
 - Datele de tranzit: securitatea retelei, schimb de mesaje, ne-repudiere
 - Serverul: securitatea serverului (serverelor), securitatea aplicatiilor, disponibilitatea serviciilor
- **Vulnerabilitate** = slabiciune a unui sistem hardware/software care permite utilizatorilor neautorizati sa aiba acces asupra lui
 - Nici un sistem nu este 100% sigur
 - Vulnerabilitati apar si datorita proastei administrari

Vulnerabilitati

- **Riscuri asociate oamenilor**

- Depasesc jumatate din tipul de atacuri in retea
- Exemplu:
 - Atacatorul foloseste *social engineering* pentru obtinerea parolei utilizator
 - Administratorul creaza sau configureaza incorect grupurile de utilizatori si drepturile lor de acces
 - Configurarea necorespunzatoare a programelor, serverelor si retelelor
 - *Bug*-uri existente in programe (introduse neintentionat deseori)
 - Ignorarea/nedocumentarea *bug*-urilor cunoscute
 - Lipsa suportului din partea producatorilor
 - Comoditatea sau necunoasterea problemelor de securitate de catre administrator ori de conducerea organizatiei
 - Angajati necinstiti care abuzeaza de politicile de acces
 - Pastrarea drepturilor pentru angajati care nu mai fac parte din organizatie
 -

Vulnerabilitati

- **Riscuri asociate transmisiilor si nivelului hardware**
 - Transmisia poate fi interceptata
 - *Man-in-middle attack*
 - Exemplu: un cracker capata acces asupra unui AP care ofera acces liber la WI-FI
 - Broadcast-ul realizat de un hub intr-un segment de retea poate fi vulnerabil la *sniffing*
 - Porturile serverelor neutilizate pot fi exploatare (solutie: *port scanner*)
 - Neconfigurarea corespunzatoare a routerelor poate permite utilizatorilor externi vizualizarea adreselor private
 - Neschimbarea suficient de des a parolelelor pentru routere si alte dispozitive
 - Accesul fizic la echipamentele retelei (servere, routere, sisteme intermediare,...)

Vulnerabilitati

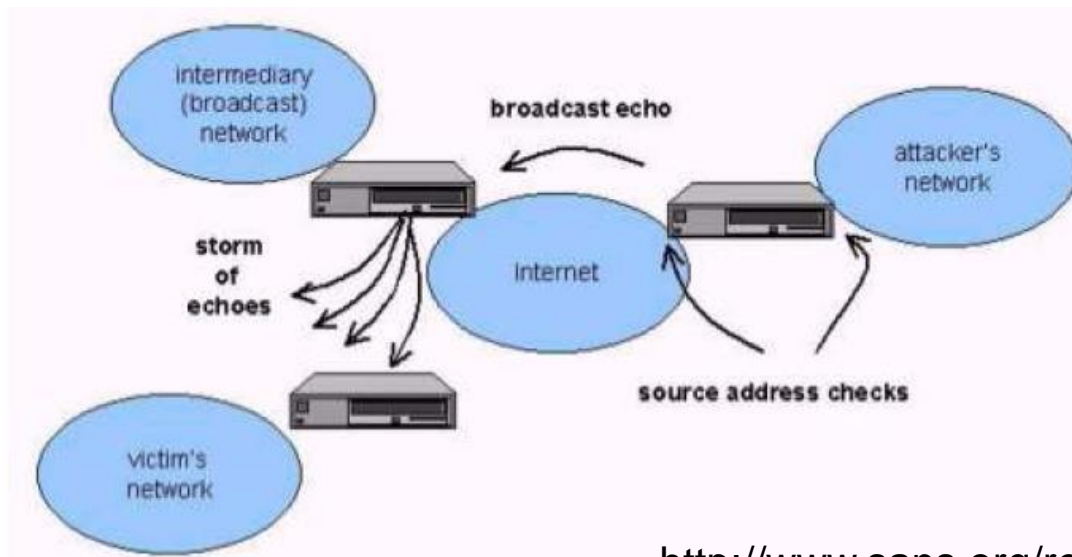
Riscuri asociate cu protocoalele si software-ul utilizat

- **Obs. Distinctia hardware vs. software este greu de facut deoarece protocoalele si nivelul hardware opereaza in tandem**
- Implementari DNS eronate
 - Vulnerabilitati BIND
- Servicii “antice” operationale
 - E.g., telnet, TFTP, ...
- Servicii/protocoale oferind date necriptate
 - FTP, SMTP, POP
- “Gauri” prezente in aplicatii (*aplication holes*)
 - Exemplificari: Apache, IIS, MSIE, Outlook, phpBB, ...
- Script-urile CGI (Common Gateway Interface)
- Existenta conturilor/configuratiilor implicite
- Permisuni inadecvate pentru fisiere, servicii, conturi-utilizator
- Lipsa mecanismelor de monitorizare & detectare a intrusilor
- Existenta exemplelor de configuratii, programe demonstrative ce pot fi exploatare

Vulnerabilitati

- **Riscuri asociate accesului la internet**

- Un firewall poate sa nu fie corespunzator configurat => obtinerea de adrese IP, ce vor fi utilizate pentru *IP Spoofing*
- Atac de tip *denial-of-service*: sistemul a devenit nefunctionabil deoarece este invadat cu transmisii de date
 - Atac de tip *smurf*: “flood of broadcast ping messages”



Exemplu: Atac de tip *smurf*

http://www.sans.org/reading_room/whitepapers/threats/icmp_attacks_illustrated_477?show=477.php&cat=threats

Atacuri

- Cunoasterea profilului atacatorului
- Atribute ce trebuie considerate
 - Resurse disponibile
(financiare, tehnice, pregatirea in domeniu,...)
 - Timpul alocat
(atacatorii rabdatori vor avea mai mult succes)
 - Riscul asumat – depinde de obiective
(atacul ar putea fi revendicat sau nu de *cracker*)
 - Accesul la Internet & calitatea acestuia: tip (*wireless*, conexiune satelit,...), mod de alocare al IP-ului
 - Obiectivele urmarite (recunoastere mondiala, denigrarea tinte, furt de informatii, furt de bani, ...)

Atacuri

- Niveluri de atac
 - **Oportunist** (*script kid*)
 - Scop “recreational”
 - Fara obiective/tinte clar definite
 - Se utilizeaza programe disponibile liber pentru a scana sau testa vulnerabilitati uzuale (e.g., software de scanare, *rootkits*,...)
 - Nu necesita acces in interiorul sistemului
 - Cunostinte vagi despre sistemul/organizatia tinta
 - Masuri de precautie:
 - Ziduri de protectie (*firewall*-uri)
 - Actualizarea versiunilor de programe

Atacuri

- Niveluri de atac

- **Intermediar**

- Obiectiv conturat, la nivelul organizatiei
 - Se vor efectua aceleasi actiuni ca la atacul “recreational”, dar se incearca ascunderea lor
 - Atacatorul are mai multa rabdare
 - Cunostinte tehnice mai profunde (uzual, la nivelul unui administrator de retea)
 - Probabilitate mai mare de succes, posibil efecte mai mari

- **Sofisticat**

- Obiectiv foarte bine conturat; Tinta este de cele mai multe ori o organizatie
 - Atacurile pot trece peste masurile de prevedere
 - Atacatorul va avea multa rabdare; Se investeste timp pentru colectarea de informatii despre sistemul/organizatia tinta
 - Foarte bune abilitati tehnice; Probabilitate mare de succes

Atacuri

| Tip atacator | Resurse | Timp | Instrumente | Risc | Acces | Obiective |
|---------------------------------|--|---|---|--|-------------------|---|
| Atacator recreațional | Cunoștințe tehnice în general limitate | De obicei oportunist | Utilizează instrumente liber disponibile | Posibil să nu înțeleagă/aprecieze riscul | Extern | Recunoaștere personală, să-și dezvolte abilitățile de cracker |
| Angajat sau fost angajat | Depinde de abilitățile personale | Poate fi răbdător și aștepta apariția unei oportunități | Utilizează instrum. liber disponibile. Dacă a fost admin., ar putea dezvolt. singur instrumente | Înțelegere a riscului, mai ales dacă este încă angajat | Intern sau extern | Avantaje personale. Denigrarea organizației |

Atacuri

| Tip atacator | Resurse | Timp | Instrumente | Risc | Acces | Obiective |
|---|------------------------------------|--|---|------------------------------------|--------|--|
| Activist cu motivație etică sau politică | Posibil să lucreze în echipă | Posibil răbdător, un evenim. poate însă determ. o acțiune rapidă | Utilizează instrumente liber disponibile | Nu este conștient de riscuri | Extern | Denigrarea organizației. Impresionarea opinii publice. Impresionarea instituțiilor guv. |
| Spion industrial | Cunoștințe avansate | Răbdător. Va încerca probabil ascunderea identității proprie | Poate modifica sau crea instrumente noi | Întelegere medie a riscului | Extern | Vânzarea inform. proprietary. Aflarea de informații despre concurență sau determinarea strategiilor organizației țintă |

Atacuri

| Tip atacator | Resurse | Timp | Instrumente | Risc | Acces | Obiective |
|---|---------------------------------|---|---|-----------------------------|--------|--|
| Atacator la nivel național (nation-state) | Poate angaja resurse importante | Răbdător, însă informațiile dorite pot fi necesare într-un timp scurt | Ar putea dezvolta instrumente specifice dacă este mare câștigul | Întelegere medie a riscului | Extern | Accesarea de informații guvernamentale sau informațiile proprietare ale unei organizații |

Atacuri

- **Tipuri de atac**

- **Accesul la nivel de utilizator**

- Atac prin acces via un cont de utilizator obisnuit sau cu privilegii superioare
 - Etape:
 - Colectarea de informatii (utilizatori, vulnerabilitati notorii, configuratii de sisteme tipice,...)
 - Exploatarea
 - Deteriorarea: acces la date importante, alterarea informatiilor, asigurarea accesului ulterior la sistem, modificarea jurnalelor de sistem
 - Solutii: eliminarea programelor, modulelor & serviciilor care nu sunt neaparat necesare, analizarea fisierelor de jurnalizare

Atacuri

- **Tipuri de atac**

- **Accesul de la distanta**

- Nu necesita acces-utilizator la sistem
 - Creaza refuzuri de servicii prin cereri incorecte, eventual cu “caderea” serviciilor prost proiectate
 - Etape:
 - Colectarea de informatii – identificarea de servicii
 - Exploatarea – trimiterea de pachete la portul gasit
 - Deteriorarea: distrugerea unui serviciu de retea, defectarea/incetinirea (temporara) a unui serviciu sa a sistemului

Atacuri

- **Tipuri de atac**

- **Accesul de la distanta la diverse aplicatii**

- Trimiterea de date invalide aplicatiilor, nu serviciilor de retea (traficul nu este afectat)
 - Exemple: SQL injection
 - Nu necesita obtinerea unui cont de utilizator
 - Etape:
 - Colectarea de informatii – identificarea aplicatiei (e.g. server sau client Web, aplicatie de birou, sistem de stocare, solutie de mesagerie, ...)
 - Exploatarea – trimiterea continutului, direct sau indirect (e.g., via e-mail sau FTP), spre aplicatie
 - Deteriorarea
 - » Stergerea/copierea fisierelor utilizatorilor
 - » Modificarea fisierelor de configuratie

Atacuri

- Tipuri de atac

- Inocularea de programe pe calculatorul utilizatorului

- Plasarea de programe *malware* (*virusi*, spioni, cai troieni, bombe, *scareware*...) – via script-uri, plugin-uri, componente ActiveX etc. Efecte:
 - Apelarea neautorizata de programe
 - Colectarea/distrugerea de resurse
 - Lansarea de atacuri spre alte sisteme
 - Crearea de usi ascunse (*traps/backdoors*)
 - Furtul identitatii utilizatorului
 -

<http://lifehacker.com/5560443/whats-the-difference-between-viruses-trojans-worms-and-other-malware>

Atacuri

- Tinta

- Organizatii publice sau guvernamentale
 - Recunoastere in rindul cracker-ilor
 - Captarea atentiei mass-mediei
 - Revendicari etice, politice,...
- Furnizori de Internet
 - Sabotarea activitatii
- Companii Private
 - Discreditare
 - Furt de informatii
 - Razbunare din partea fostilor angajati
- Persoane Fizice
 - Cu scop “recreational”

Atacuri

- **Moduri de atac**

- Spargerea sau penetrarea (*cracking*)

- Actiunea de descoperire a unor vulnerabilitati si de profitare de pe urma acestora
 - Acces neautorizat la sistem efectuat de *cracker*
 - Accesare, fara alta actiune – rol pasiv
 - Accesare cu alterare/distrugere a informatiilor – activ
 - Accesare cu control asupra sistemului; uneori cu creare de “usi din spate” (backdoors) – rol activ
 - Nu se acceseaza sistemul, ci se realizeaza actiuni distructive de refuz al serviciilor

Atacuri

- **Moduri de atac**

- *E-mail bombing*

- Trimiterea repetata a unui mesaj (de dimensiuni mari) spre o adresa e-mail a unui utilizator
 - Incetinesc traficul, umple discul
 - Unele atacuri pot folosi adrese e-mail multiple existente pe serverul tinta
 - Se poate combina cu falsificarea adresei (*e-mail spoofing*)

- *E-mail spamming*

- Trimiterea de mesaje nesolicitate (reclame)
 - Adresa expeditorului este falsa
 - Efectul atacului este accentuat daca mesajul va fi trimis pe o lista de discutii

Atacuri

- **Moduri de atac**

- **Abonarea la liste de discutii**

- “Atac” ce determina enervarea victimei, facilitat de diverse programe disponibile in Internet
 - Cauzeaza trafic inutil in retea

- **Flasificarea adresei expeditorului (*e-mail spoofing*)**

- Folosita pentru ascunderea identitatii expeditorului sau pentru determinarea utilizatorului sa raspunda la atac ori sa divulge informatii (e.g. parole)
 - Slabiciune datorata protocolului SMTP
 - Utilizatorii trebuie educati sa nu raspunda expeditorilor necunoscuti si sa nu divulge informatii confidentiale

Atacuri

- **Moduri de atac**

- *Social engineering*

- Manipularea utilizatorilor de catre un *craker* – *phishing* (*preluarea identitatii*)
 - Tipuri: intimidare, santaj, presiune, autoritate, flatare, substitutie de persoana, vanitate etc.
 - Atacatorul colecteaza date privitoare la persoana si/sau organizatia vizata si aplica principii de persuasiune
 - <http://www.securityfocus.com/infocus/1527>

Atacuri

- **Moduri de atac**

- **Refuzul serviciilor (*Denial Of Service*)**

- Obiectiv: Degradarea calitatatii functionarii unor servicii sau dezafectarea lor
 - Modalitate: supraincarcarea serverului sau a retelei
 - Consumarea resurselor *host*-ului
 - *flood*-uri TCP SYN
 - *flood* ICMP ECHO (ping)
 - Consumarea latimii de banda
 - *flood* UDP
 - *flood* ICMP

Atacuri

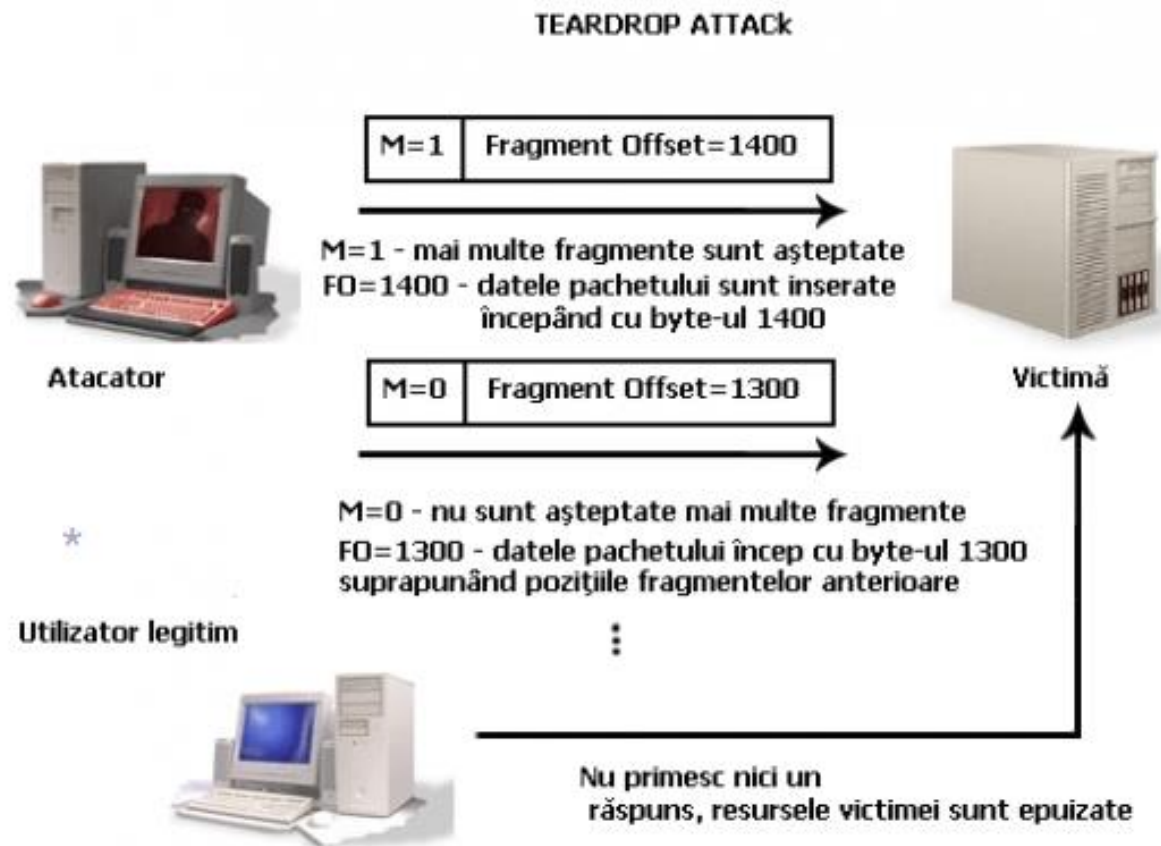
- **Moduri de atac**

- **Refuzul serviciilor (*Denial Of Service*)**

- De obicei, atacatorul isi falsifica adresa sursa (*IP spoofing*)
 - Se pot modifica porturile sursa/destinatie (pentru a trece de *firewall*-uri)
 - Exemple:
 - SYN flood – cereri multiple de realizarea a conexiunii
 - *Ping of death* – atac cu pachete ICMP mari
 - *Teardrop* – exploatarea in general al implementarilor TCP/IP care nu gestioneaza corect pachetele IP (versiunile de Windows 3.1x, Windows 95, windows NT si versiuni Linux (inainte de 2.0.32))
 - *Smurf* – atac ICMP asupra adresei de broadcast

Atacuri

- Moduri de atac
 - Teardrop



http://www.dlsit.ro/articole/106_Atacul-Teardrop

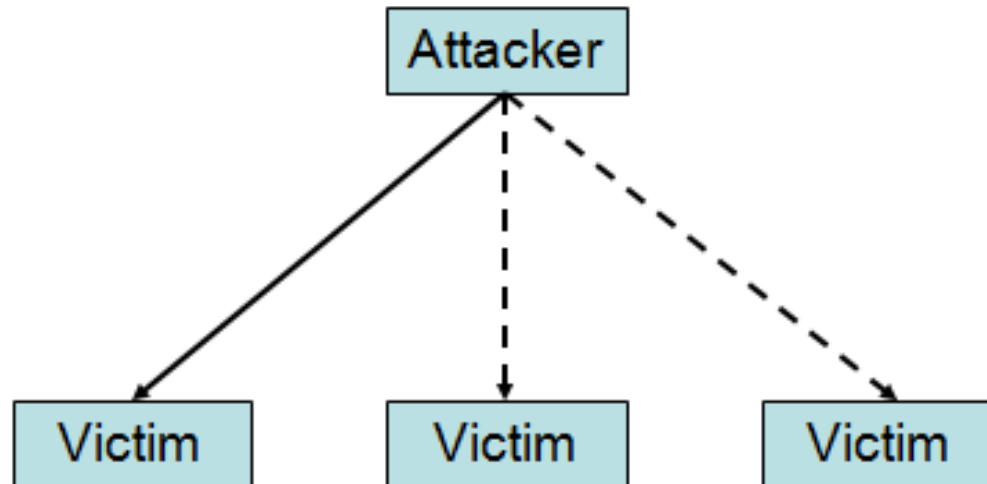
Atacuri

- **Moduri de atac**

- **Refuzul serviciilor (*Denial Of Service*)**

- DoS simplu**

- De obicei, atacatorul isi falsifica adresa sursa (*IP spoofing*)
 - Usor de rezolvat



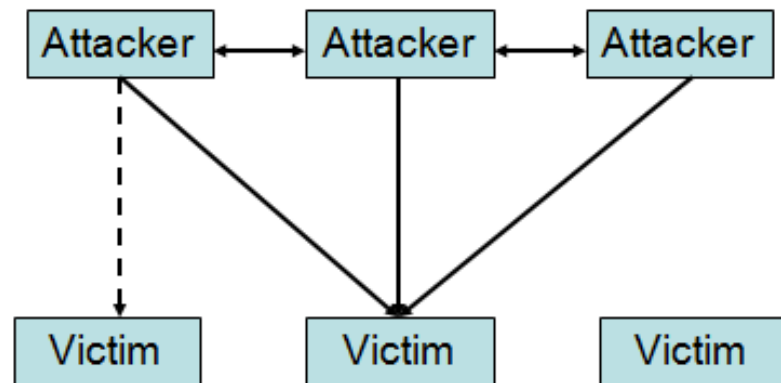
Atacuri

- Moduri de atac

- Refuzul serviciilor (*Denial Of Service*)

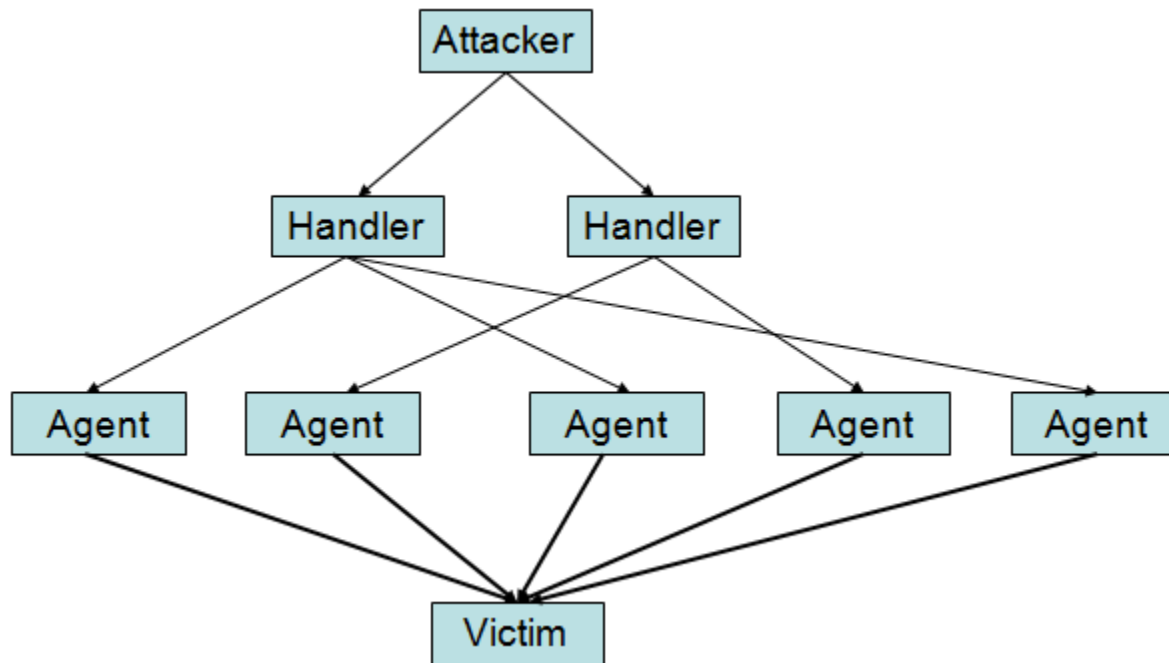
- DoS coordonat

- La primul pas, este atacata o alta victima pentru a se ascunde adevaratul atac
 - Atacatorul isi ascunde de obicei adresa de origine
 - Greu de rezolvat



Atacuri

- Moduri de atac
 - Refuzul serviciilor (*Denial Of Service*)
DDoS (*Distributed DoS*)



Atacuri

- **Moduri de atac**

- Refuzul serviciilor (*Denial Of Service*)

- DDoS (*Distributed DoS*)

- *Handlers* – sunt de obicei serverele puternice (care ascund usor pachetele de atac)
 - *Agents* – sunt de obicei utilizatori ce au computerele infectate
 - Foarte dificil de depistat atacatorul
 - Este diferit de *FlashCrowd*

- » Slashdot Effect, Victoria Secret Webcast

- (<http://www2.research.att.com/~bala/papers/www02-fc.html>)

Atacuri

- **Moduri de atac**

- **Depasirea capacitatii buffer-elor (*buffer overflow*)**

- Unele programe pot alocă spațiu insuficient pentru unele date, depășirile survenite pot produce executarea de comenzi ca utilizator privilegiat (root)
 - Unele funcții C – precum `gets()`, `getwd()`, `strcpy()`, `strcat()` – oferă premisele apariției de *buffer overflow*-uri
 - Exemple: suprascriere de cod, alterarea stivei de pointeri
 - Uzual atacul provine din interior, dar poate fi și din exterior (via un cal troian)

Atacuri

- **Moduri de atac**

- **Interceptarea rețelei (*IP sniffing*)**

- Monitorizarea datelor care circula printr-o interfata de retea
 - Se pot detecta parole transmise necriptate
 - Atacul provine din interior
 - Pentru rețele de mare viteză (peste 100M/s) unele pachete nu pot fi captate de *sniffer*
 - Software-ul interceptor trebuie supravegheat
 - Exemple: tcpdump, Wireshark (Ethreal)

Atacuri

- Moduri de atac

- Virusi

- Programe ce efectueaza operatii nedorite (distructive), cu capacitati de “multiplicare”
 - Infectarea altor programe (uzual, executabile)
 - Mai putin raspinditi in Unix/Linux, de obicei avind efect doar daca se executa sub auspicii de *root*
 - Pot genera si *e-mail bombing*
 - Remedii: utilizarea de antivirusi si porti de *e-mail*

Atacuri

- **Moduri de atac**

- **Cai troieni (trojan horses)**

- Programe rau intentionate “deghizate sub forma unor executabile “utile”
 - Apeleaza programe neautorizate sau sunt modificate, incluzind cod nelegitim
 - Actiuni: colectarea de informatii, distrugerea de informatii, lansarea de atacuri spre alte sisteme
 - Exemple: “vaduva neagra” (blocheaza sau corupe browsere Web)

Atacuri

- **Moduri de atac**

- **Usi ascunse (back doors/ traps)**

- Caz particular de cai troieni
 - Creaza o “poarta” (e.g. utilizator, port,...) care permite accesul ulterior la calculator si/sau castigarea de privilegii

- **Viermi (worms)**

- Programe care se multiplica, transferindu-se pe alte gazde si efectuind (eventual) distrugeri
 - Exemplu celebru: Internet Worm (Morris Worm) (1988)
 - *fork bomb effect*

Atacuri

- **Moduri de atac**

- **Ghicirea parolelor (*password guessing*)**

- Majoritatea proceselor de autentificare folosesc parole
 - Cu cat utilizatorul trebuie sa retina mai multe parole, cu atat sistemul de protectie via parole este predispus la brese in securitate:
 - Alegerea unor parole slabe
 - Partajarea parolelor (colegi, prieteni,...)
 - Scrierea parolelor pe hirtie
 - Folosirea aceleiasi parole timp indelungat, pentru mai multe aplicatii/sisteme
 - Folosirea unui program ce determina parolele prost alese (prea simple, prea scurte, cuvinte din dictionar,..)
 - Protectie prin /etc/shadow, reguli stricte de schimbarea parolelor, educarea utilizatorilor
 - Alte solutii: SSO (Single Sign On), identificare biometrica etc

Atacuri

- **Moduri de atac**

- **Utilizarea tehnicilor de *reverse code-engineering***

- Analiza aplicatiilor binare fara cod-sursa accesibil (*closed –source*), pentru a se observa modul de executie la nivel scazut
 - Folosita si pentru a studia codul *malware*
 - Instrumente: editoare hexa, dezasambloare, depanatoare, monitoare de sistem,...
 - Apar probleme de legalitate

Prevenirea

- La ce nivel trebuie luate masuri de securitate?
 - Nivel fizic: inhibarea ascultarii mediilor de transmisie, interzicerea accesului fizic la server, ...
 - Nivelul legatura de date: criptarea legaturii
 - Nivelul retea: ziduri de protectie (*firewall-uri*)
 - Nivelul transport: criptarea conexiunilor (SSL – *Secure Socket Layer*, TLS – *Transport Layer Security*)
 - Nivelul aplicatiei: monitorizare si actualizarea software-ului, jurnalizare, educarea utilizatorilor, politici generale adoptate,...

Prevenirea

- **Elaborarea de politici de securitate**
 - Planificarea cerintelor de securitate (confidentialitate, integritate, disponibilitate,...)
 - Evidentierea riscurilor
 - Scenarii de risc
 - Analiza raportului cost-beneficii
 - Costurile prevenirii, refacerii dupa dezastru etc.
 - Stabilirea politicilor de securitate
 - Politica generala (nationala, organizationala,...)
 - Politici separate pentru diverse domenii protejate
 - Standarde & reglementari (recomandari)

Prevenirea

- **Elaborarea de politici de securitate - exemplu**
 - Gestionarea accesului (nume de cont, modul de schimbare a parolei, politica de acces din exterior,...)
 - Clasificarea utilizatorilor (grupuri, permisiuni, utilizatori speciali, utilizatori administratori,...): ACL (Access Control List)
 - Accesul la resurse (drepturi de acces la fisiere, directoare, criptarea fisierelor importante,...)
 - Monitorizarea activitatii (fisiere de jurnalizare)
 - Administrarea copiilor de siguranta (tipuri de salvari, medii de stocare, durata pastrarii, ...)

Prevenirea

- Principii de baza

- Simplificare – configurarea sistemului astfel incat sa acorde vizitatorilor cele mai scazute privilegii
 - Reducere – minimizarea ariei de actiune
 - Intarire – “never trust user input” + securizarea accesului la fisiere/aplicatii externe
 - Diversificare – utilizarea mai multor niveluri de protectie (fara *security through obscurity*)
 - Documentarea – memorarea setarilor, strategiilor si masurilor adoptate pentru securitate
- Obs. Siguranta sistemului depinde de cea mai vulnerabila componenta a acestuia

Supravietuirea

- **Supravietuirea** = capacitatea unui sistem (calculator/retea) de a-si indeplini misiunea, in timp util, in prezenta atacurilor, defectelor sau accidentelor
- **Atac** = eveniment potential distrugator provocat intentionat de persoane rau-voitoare
- **Defect** = eveniment potential distrugator cauzat de deficiente ale sistemului sau ale unui factor de care depinde sistemul (e.g., defecte hardware, bug-uri software, erori ale utilizatorilor)
- **Accident** = evenimente neprevazute (e.g. dezastre naturale, caderi de tensiune,...)
- Sistemul trebuie sa sustina macar indeplinirea functiilor vitale (*mission-critical*)
 - Identificarea serviciilor esentiale,
 - Identificarea perimetrilor de securitate majora

Supravietuirea

- **Proprietati ale sistemului:**
 - **Rezistenta la atacuri** = strategii de respingere a atacului (e.g. autentificarea utilizatorilor, *firewall*-uri, validarea obligatorie a datelor de intrare)
 - Recunoasterea atacurilor si efectelor lor = strategii pentru restaurarea informatiilor, limitarea efectelor, mentinerea/restaurarea serviciilor compromise
RAID (Redundant Array of Independent Disks),
SAN (Storage Area Network), backup-uri, cluster-e,...)
 - Adaptarea la atacuri = strategii pentru imbunatatirea nivelului de supravietuire -> invatarea din greseli

Monitorizarea

- **Monitorizarea securitatii retelei (NSM – Network Security Monitoring)** = colectarea, analiza si aprecierea indicatorilor si avertismentelor privind **detectarea** si **raspunsul** la incidente de securitate
 - **Indicator**: actiune observabila care confirma intentiile sau capacitatile de atac
 - Indicatorii generati de sistemele de detectie a intrusilor se mai numesc si **alerte** (vizind un anumit **context**)
- Observatii:
 - Detectarea este realizata (automat) de produse software
 - Analizarea implica factori umani
 - Aprecierea incidentului reprezinta un proces de luare a deciziilor

Monitorizarea: detectarea

- **Principii:**

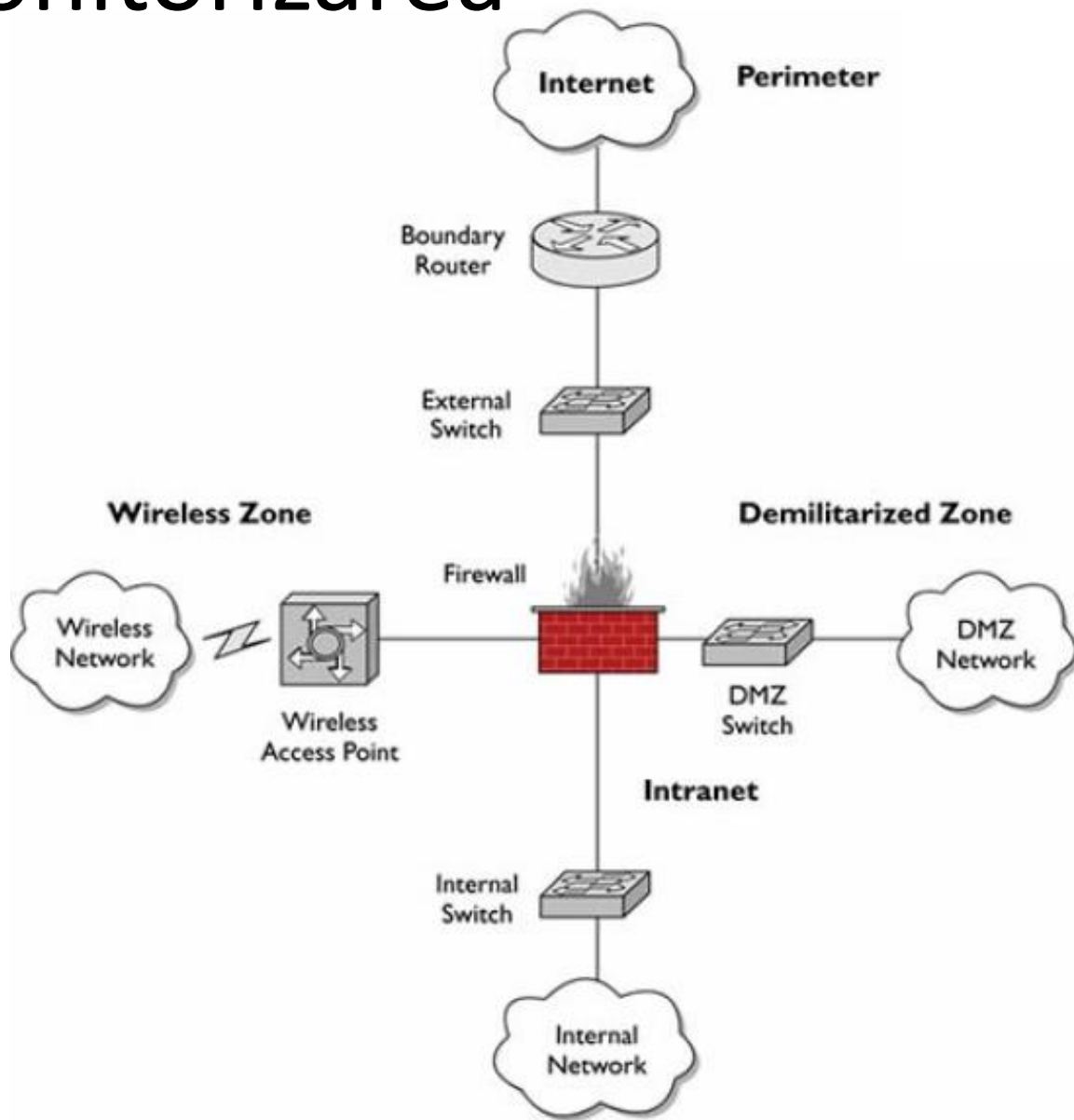
- Intrusii care comunica (direct/indirect) cu victimele pot fi detectati
- Detectia prin luare de probe (*sampling*) este superioara lipsei de detectie (Nu pot fi monitorizate toate datele)
- Detectia pe baza analizei traficului este superioara lipsei detectiei

- Obs.

- Colectarea tuturor datelor este problematica
- Colectarea datelor poate fi efectiva daca se bazeaza pe aparitia unor evenimente
- Instrumentele de detectie trebuie sa fie optimizate si trebuie sa asigure ergonomia utilizatorului

Monitorizarea

- Divizarea rețelei în zone de interes
 - Fiecare zonă poate fi tinta unor atacuri
 - DMZ separa datele sensibile de cele disponibil public



Monitorizarea

- Pot fi colectate date provenite de la:
 - *Hub-uri*, porturile *switch-urilor* (via **SPAN – Switched Port Analyzer**), *tap-uri* (*test access port* – dispozitiv de retea proiectat special pentru monitorizare), portile de filtrare (*filtering bridges*) – pentru rețele cu fir
 - Senzori între *firewall-ul* organizației și punctul de acces *wireless*, o platforma *wireless* – pentru rețele *wireless*
- Realizarea de statistici
 - La nivel de router (e.g. *CISCO accounting*)
 - La nivel de sistem de operare
 - Instrumente: *lpcad*, *ifstat*, *tcpdstat*, *MRTG* (Multi Router Traffic Grapher) etc.

Monitorizarea: identificarea

- Date (trafic de retea)
 - Normale
 - Privind HTTP, FTP, SMTP, POP3, DNS, IP, SSL/TLS etc
 - Suspicioase
 - Apar dubioase la prima vedere, dar nu cauzeaza probleme pentru corporatie, ci eventual doar utilizatorului
 - Malitioase
 - Au impact negativ asupra securitatii organizatiei

Monitorizarea: validarea

- Validarea asociaza un incident preliminar unei categorii de evenimente:
 - Acces neautorizat ca *root* (administrator)
 - Acces neautorizat la nivel de utilizator
 - Incercare de accesare neautorizata
 - Atac (D)Dos soldat cu succes
 - Violare a politicii de securitate
 - Scanare, probare, detectie
 - Infectie cu virusi

Monitorizarea: reactia

- Dupa aparitia unui incident de securitate, trebuie demarata o reactie:
 - Pe termen scurt – STIC (*SHORT-Term Incident Containment*)
 - Exemplu: inchiderea portului *switch*-ului prin care se realizeaz atacul, deconectarea fizica, introducerea unei reguli noi de filtrare a datelor etc.
 - Intrarea in stare de urgenta
 - O importanta majora o are analiza (*analyst feedback*) ->Implica personal specializat

Monitorizarea

- Se poate recurge si la capcane pentru *craker*-i: *honeypots*
 - Masini-tinta special configurate pentru a observa atacurile *cracker*-ilor
 - Mai multe *honeypots* formeaza un *honeynet* (<http://www.honeynet.org>)
 - Pentru a detecta & studia noi tehnici de atac si pentru a contracara diverse incidente de securitate
 - Folosind un daemon (*honeyd*), se pot imita servicii de retea, rulind intr-un mediu virtual

Testarea

- Teste de verificare a:
 - Capacitatii de deservire a clientilor
 - Robustetei
 - Rularii in situatii extreme
- Teste referitoare la performante
- Teste specifice legate de exploatare
 - Pregatirea adecvata a exploatarii in practica (*deployment*)
 - Teste de incarcare (*load testing*)
- Teste privind opacizarea datelor (*obfuscation*)
 - Datele nu trebuie stocate in locatii predictibile
- Teste privitoare la integrarea componentelor
- Teste specifice legate de programare (ex. Lungimea parametrilor trimisi de client, a interogarilor SQL, etc)

Testarea

- Instrumentele de stresare (*stressing tools*) pot da informatii privitoare la:
 - Performanta (timp de raspuns, timp de generare a continutului etc.)
 - Scalabilitate (memoria ocupata, utilizarea discului, numarul inregistrarilor inserate, accesarea altor tipuri de resurse, ...)
 - Corectitudine (functionarea eronata a unor componente)
 - Lacune de securitate
- Metodologii de analiza a riscurilor: **DREAD** (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability), **OCTAVE** (Operationally Critical Threat Asset and Vulnerability Evaluation), **STRIDE** (Spoofing identity, Tempering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege), **OSSTMM** (open Source Security Testing Methodology Manual) – www.ostmm.org

Testarea

- **SANS** (System Administration, Networking, and Security) :
 - Pregătire
 - Identificare
 - Controlul efectelor
 - Eradicare
 - Recuperare
 - Continuare (*follow-up*)
- Raspunsurile agresive sunt prohibite! (*hack back*)
- *Forensics* = procesul de “prindere” a cracker-ilor
 - Uzual, are loc dupa un incident de securitate
 - Implica: analiza hardware-ului (discuri, RAM,...), log-urilor etc.
 - Instrumente: WinHex, FIRE (forinsec and Incident Response Environment), ForensiX

Protocoloale – exemple

- **Nivelul retea**

IPSec – RFC 2401, 2402, 2406, 2408

- Servicii oferite: controlul accesului, integritatea datelor, autentificare, confidentialitate
- Poate fi implementat in cadrul unui *router* sau *firewall*
- Nu necesita modificarea software-ului la nivel de transport/aplicatie
- Autentificarea & integritatea se precizeaza intr-un antet special: Authentication Header
- Confidentialitatea este asigurata de algoritmi de criptare via date suplimentare

ESP (*Encapsulating Security Payload*)

Protoacoale – exemple

- **Nivelul transport**

TLS (Transport Layer Security) – RFC5246 (TLS 1.2)

- Imbunatatire a SSL (Secure Socket Layer) creat de Netscape

SSL(Secure Sockets Layer)

- Metoda de criptare a transmisiilor TCP/IP (e.g. pagini Web, date introduse in *form-uri* web) - HTTP over Secure Sockets Layer or HTTP Secure
- Oferă servicii de securitate de baza pentru TCP
- Fiecare conexiune dintre un client si server reprezinta o sesiune (*session*)
- Starea unei sesiuni = identificator unic al sesiunii, certificat digital, metoda de compresie, metoda de cifrare (algoritm de criptare sau de tip hash), cod secret partajat de client & server
- Un mesaj are asociat un cod de autentificare: MAC (Message Authentication Code)

Protoacoale – exemple

- **Nivelul transport**

TLS (Transport Layer Security) – RFC5246 (TLS 1.2)

- **Alert Protocol** – mecanism care permite managementul alertelor provenite de la un punct terminal: mesaj neasteptat receptionat, eroare de decompresie, MAC incorect, certificat eronat
- **Handshake Protocol** – permite autentificarea serverului la client si vice-versa, plus negocierea algoritmilor de criptare si a cheilor; se realizeaza inainte de transmiterea efectiva a datelor

Protocoloale – exemple

- **Nivelul aplicatie**

SSH (Secure Shell)

- negociaza si stabileste o conexiune criptata intre un server si un client SSH via metode diverse de autentificare
- Implementari: ssh, PuTTY, SCP (*Secure CoPy*),...

PCP (Pretty Good Privacy) – RFC 3156

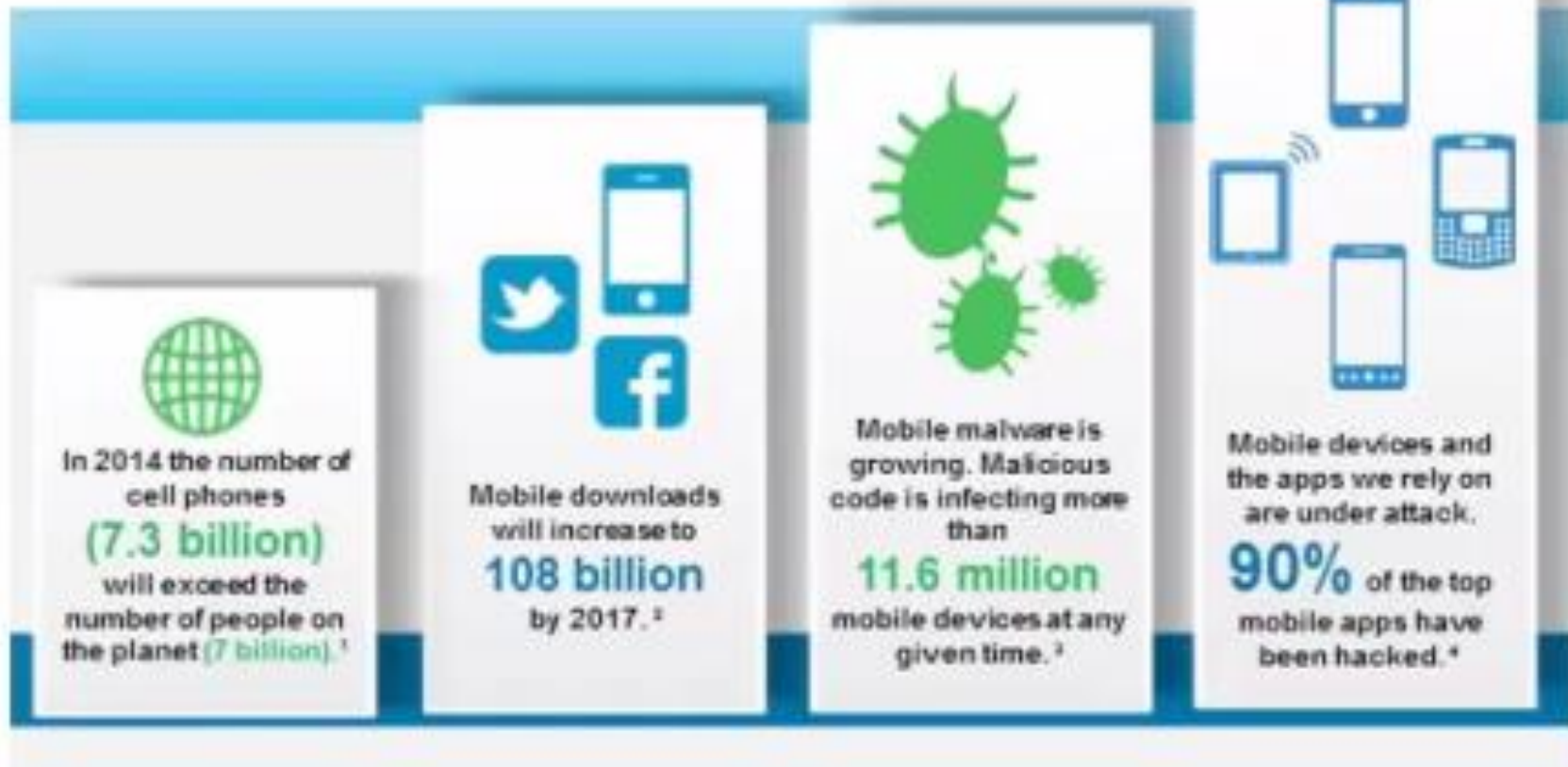
- Oferă confidențialitate & autentificarea mesajelor e-mail și a fișierelor transmise prin rețea
- Folosește o pleiadă de algoritmi de criptare
- Implementari: GPG (GNU Privacy Guard)

S/MIME – RFC 3369, 3370, 3850, 3851

- Pune la dispoziție extensii de securitate pentru MIME (Multipurpose Internet Mail Extension)

Atacuri

AS MOBILE GROWS, SO DO SECURITY THREATS



Atacuri

- Atacuri la nivel *wireless*
 - Diminuarea semnalului
 - Capturarea pachetelor de date (*wireless sniffing*)
 - Atacuri asupra WEP (Wired Equivalent Privacy)
 - Crearea de virusi/ cod malitios
 - Folosirea resurselor retelelor wireless publice sau ale unor companii
 - *Snooping* (accesarea datelor private)
 - *Masquerading* (furt de identitate al unui dispozitiv)
 - DoS (refuz al serviciilor)

Probleme specifice

- **Sistemele wireless**
 - Necesitate: un mediu sigur (autentificare, integritate a datelor, confidentialitate, autorizare, nerepudiere)
 - Pericole – tipuri de atacuri:
 - Falsificarea identitatii (*spoofing*)
 - Interceptarea (*sniffing*)
 - Alterarea datelor (*tampering*)
 - Interferenta (*jamming*) – e.g. la Bluetooth
 - Furtul (*device theft*)

Probleme specifice

- **Sistemele wireless**

- Solutii:

- WEP (Wired Equivalent Privacy) – standard vechi inlocuit in 2003 de WPA
- WPA (WI-FI Protected Access) – subset al 802.11i – foloseste metoda de criptare diferita (RC4 fata de AES), WPA2
- Protocoale de securitate WTLS (Wireless Transport Layer Security)
- Securitatea la nivel IP: IPSec
- Extensii de securitate in cadrul IP-ului mobil
- Firewall-uri
- ...

Statistic

Top atacuri in 2016: <https://securelist.com/analysis/kaspersky-security-bulletin/76858/kaspersky-security-bulletin-2016-executive-summary/>

- **xDedic – the shady marketplace** – *“facilitated the buying and selling of hacked server credentials. Around 70,000 compromised servers were on offer – although later [evidence](#) suggests that there could have been as many as 176,000 – located in organisations around the world”*
- In February 2016, hackers used the **SWIFT** credentials of Bangladesh Central Bank employees to send fraudulent transaction requests to the Federal Reserve Bank of New York, asking it to transfer millions of dollars to various bank accounts in Asia. The hackers were able to get \$81 million transferred to the Rizal Commercial Banking Corporation in the Philippines and an additional \$20 million to Pan Asia Banking.
 - Society for Worldwide Interbank Financial Telecommunication (SWIFT) provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardized and reliable environment. SWIFT also sells software and services to financial institutions, much of it for use on the SWIFTNet Network
- ...
<http://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/>

Statistici

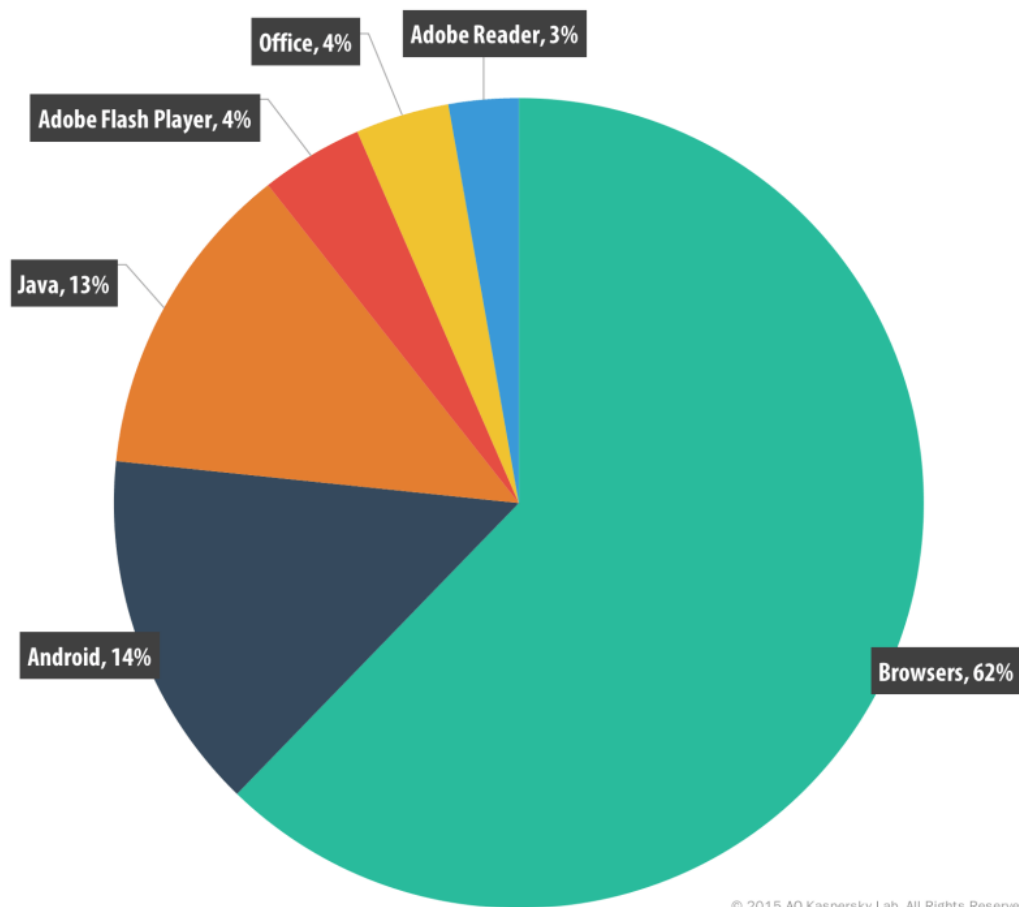
Top atacuri in 2016: <https://securelist.com/analysis/kaspersky-security-bulletin/76858/kaspersky-security-bulletin-2016-executive-summary/>

- In October, attackers used a botnet of over half a million internet-connected home devices to launch a [DDoS attack against Dyn](#) – a company that provides [DNS](#) services to Twitter, Amazon, PayPal, Netflix and others. The world was shocked, but warnings about unstable IoT security have been around for a long time....

<http://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/>

Statistici

Perioada 2015
Top aplicatii vizate de
Atacatori (inclusiv
pentru
dispozitivele mobile)



<http://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/>

Top 10 programe malitioase

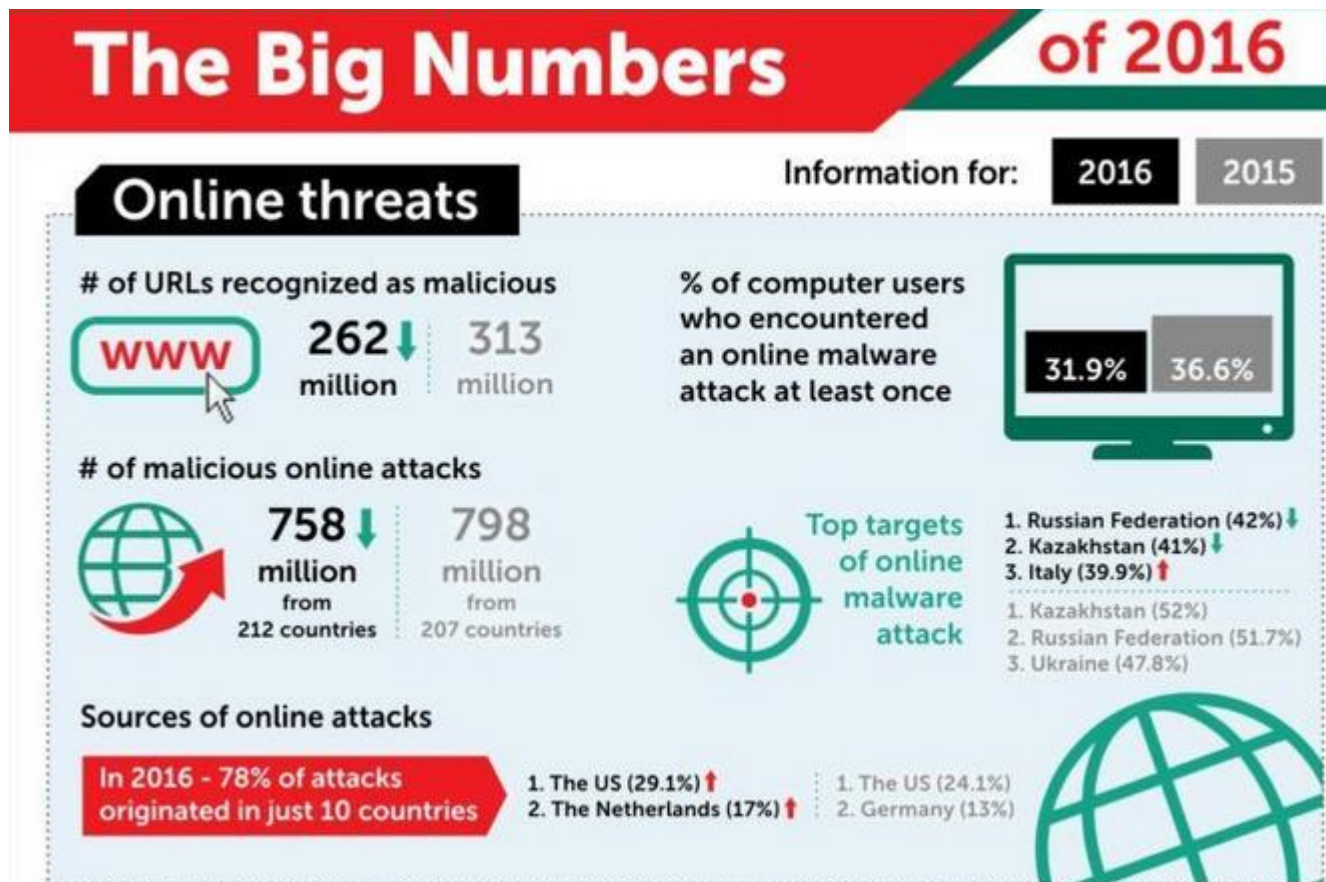
| | Name | Verdicts* | percentage of users** |
|----|-----------------------------------|---|-----------------------|
| 1 | CTB-Locker | Trojan-Ransom.Win32.Onion / Trojan-Ransom.NSIS.Onion | 25.32 |
| 2 | Locky | Trojan-Ransom.Win32.Locky / Trojan-Dropper.JS.Locky | 7.07 |
| 3 | TeslaCrypt (active till May 2016) | Trojan-Ransom.Win32.Bitman | 6.54 |
| 4 | Scatter | Trojan-Ransom.Win32.Scatter / Trojan-Ransom.BAT.Scatter / Trojan-Downloader.JS.Scatter / Trojan-Dropper.JS.Scatter | 2.85 |
| 5 | Cryakl | Trojan-Ransom.Win32.Cryakl | 2.79 |
| 6 | CryptoWall | Trojan-Ransom.Win32.Cryptodef | 2.36 |
| 7 | Shade | Trojan-Ransom.Win32.Shade | 1.73 |
| 8 | (generic verdict) | Trojan-Ransom.Win32.Snocry | 1.26 |
| 9 | Crysis | Trojan-Ransom.Win32.Crusis | 1.15 |
| 10 | Cryrar/ACCDFISA | Trojan-Ransom.Win32.Cryrar | 0.90 |

According to [Kaspersky Lab research](#), in 2016, one in every five businesses worldwide suffered an IT security incident as a result of a ransomware attack.

- 42% of small and medium-sized businesses were hit by ransomware in the last 12 months.
- 32% of them paid the ransom.
- One in five never got their files back, even after paying.
- 67% of those affected by ransomware lost part or all of their corporate data – and one- in-four spent several weeks trying to restore access.

| | Industry sector | % attacked with ransomware |
|----|--------------------------------------|----------------------------|
| 1 | Education | 23 |
| 2 | IT/Telecoms | 22 |
| 3 | Entertainment/Media | 21 |
| 4 | Financial Services | 21 |
| 5 | Construction | 19 |
| 6 | Government/ public sector/defence | 18 |
| 7 | Manufacturing | 18 |
| 8 | Transport | 17 |
| 9 | Healthcare | 16 |
| 10 | Retail/wholesale/leisure | 16 |

Statistică



<https://securelist.com/analysis/kaspersky-security-bulletin/76858/kaspersky-security-bulletin-2016-executive-summary/>

Statistici

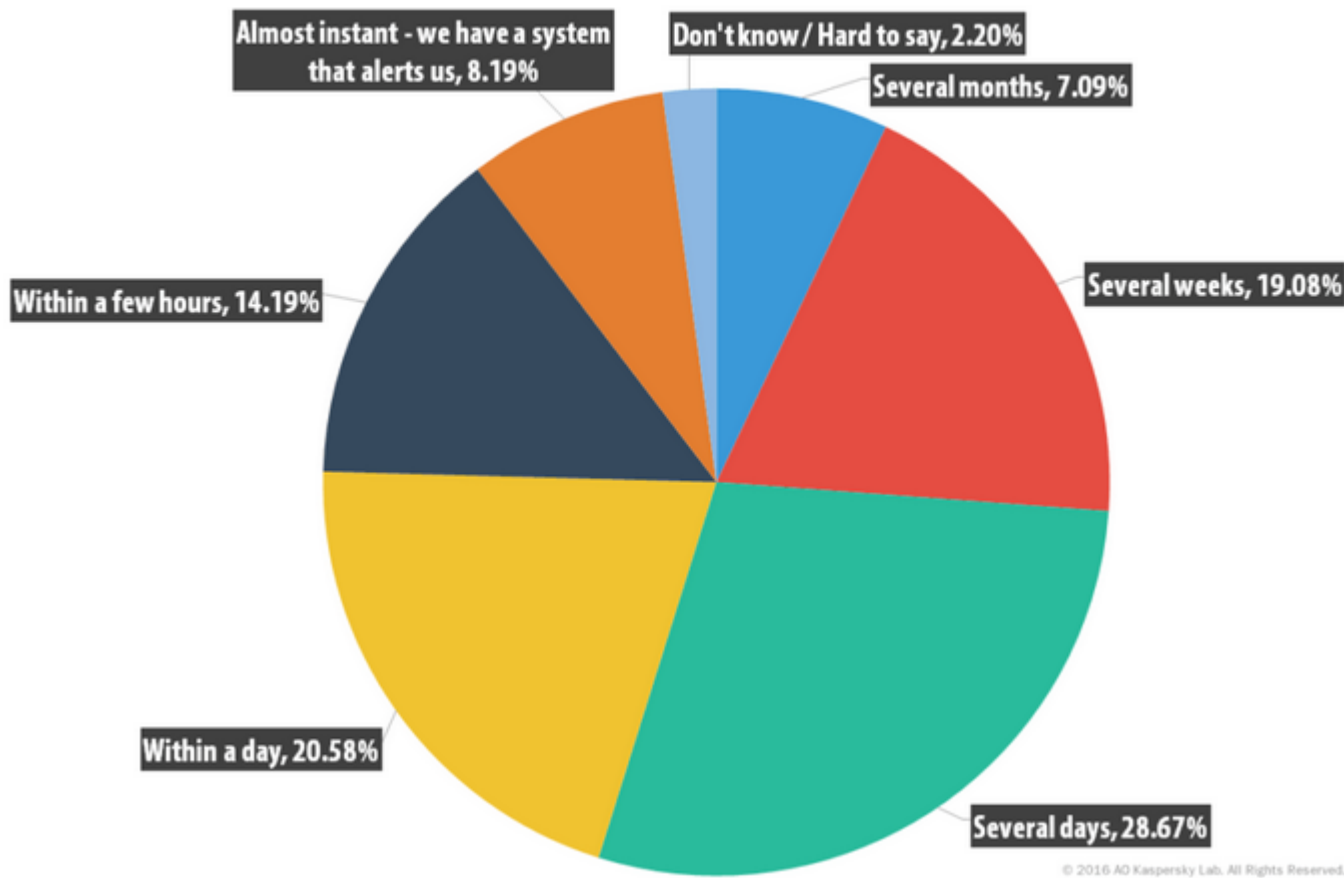
Perioada 2016



<https://securelist.com/analysis/kaspersky-security-bulletin/76858/kaspersky-security-bulletin-2016-executive-summary/>

Statistici

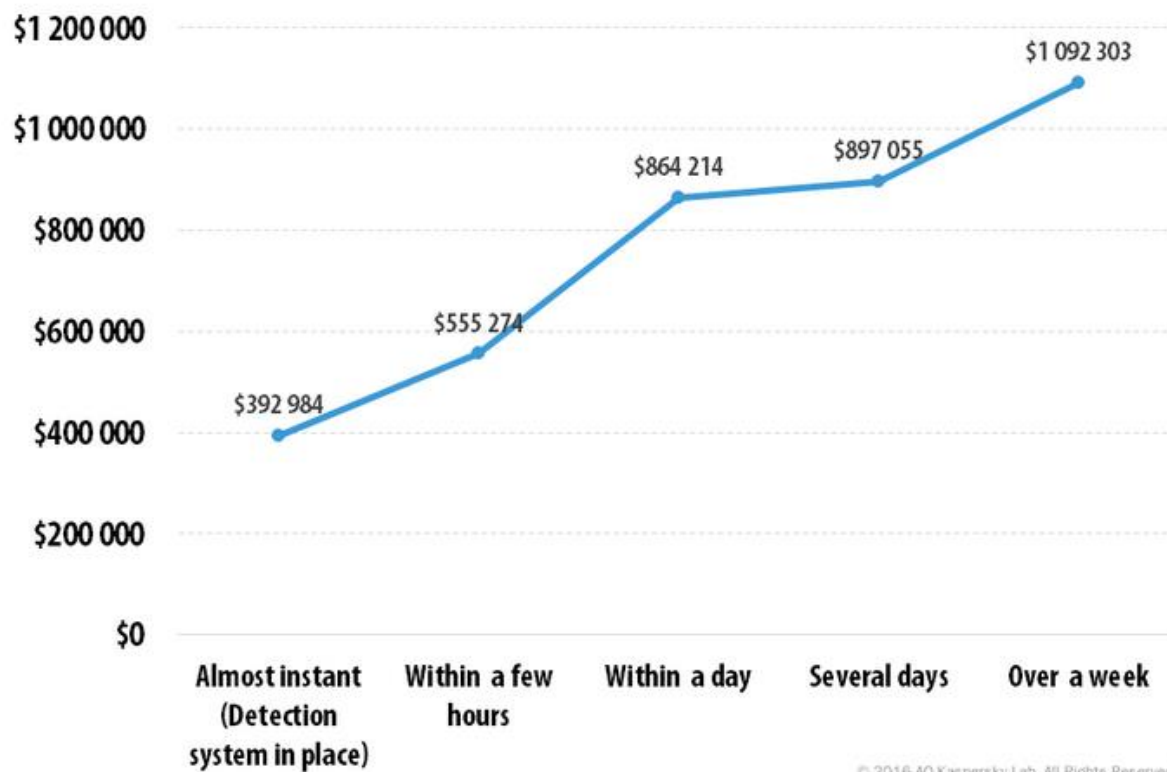
Timpul de detectare al incidentelor de securitate - Statistici



<https://securelist.com/analysis/kaspersky-security-bulletin/76858/kaspersky-security-bulletin-2016-executive-summary/>

Statistici

Timpul de detectare al incidentelor de securitate – Statistici&Costuri



Cost of recovery vs. time needed to discover a security breach for enterprises

<https://securelist.com/analysis/kaspersky-security-bulletin/76858/kaspersky-security-bulletin-2016-executive-summary/>

Previziuni -2017

- *1. Ransomware attacks will decrease in volume and effectiveness in the second half of 2017.*
- *2. Windows vulnerability exploits will continue to decline, while those targeting infrastructure software and virtualization software will increase.*
- *3. Hardware and firmware will be increasingly targeted by sophisticated attackers.*
- *4. Hackers using software running on laptops will attempt “dronejackings” for a variety of criminal or hacktivist purposes.*
- *5. Mobile attacks will combine mobile device locks with credential theft, allowing cyber thieves to access such things as banks accounts and credit cards.*
- *6. IoT malware will open backdoors into the connected home that could go undetected for years.*
- *7. Machine learning will accelerate the proliferation of and increase the sophistication of social engineering attacks.*
- *8. Fake ads and purchased “likes” will continue to proliferate and erode trust.*
- *9. Ad wars will escalate and new techniques used by advertisers to deliver ads will be copied by attackers to boost malware delivery capabilities.*
- *10. Hacktivists will play an important role in exposing privacy issues.*
- *11. Leveraging increased cooperation between law enforcement and industry, law enforcement takedown operations will put a dent in cybercrime.*
- *12. Threat intelligence sharing will make great developmental strides in 2017.*
- *13. Cyber espionage will become as common in the private sector and criminal underworld as it is among nation-states.*
- *14. Physical and cybersecurity industry players will collaborate to harden products against digital threats.*

<http://www.securitymagazine.com/articles/87628-threat-trends-to-watch-in-2017>

Rezumat

- Preliminarii
- Aspecte importante
- Vulnerabilitati
- Atacuri
- Prevenirea si supravietuirea
- Monitorizarea
- Testarea
- Raspunsul la incidente
- Protocoale
- Probleme specifice
- Statistici & Previziuni

Bibliografie

- Security guide to network security fundamentals, Mark Ciampa, 2009
- Network+ Guide to Networks, Fifth Edition, Tamara Dean, Network +, ISBN-13: 978-1-423-90245-4, 2009
- <http://www.scribd.com/doc/55573866/57/Func%C5%A3iile-Hash>
- http://www.lsec.be/upload_directories/documents/2011/sophos-security-threat-report-2011-wpna.pdf
- <http://securelist.com/statistics/>
- <https://securelist.com/analysis/kaspersky-security-bulletin/73038/kaspersky-security-bulletin-2015-overall-statistics-for-2015/>
- http://www.dlsit.ro/articole/106_Atacul-Teardrop
- <https://brighttalkservices.app.box.com/s/ym2v7t9bbuchnj53gmrtd6g4uinbb59u>



Intrebari?

“Little by little, one travels far.”
(J. R. R. Tolkien)