Noţiuni de bază în securitate – nivele minime de securitate acceptabile

Fişa de documentare 1.1 Noţiuni de securitate a sistemelor de calcul

Acest material vizează competenţa/rezultat al învăţării: **Identifică fundamentele şi principiile securităţii sistemelor de calcul şi a reţelelor de calculatoare**

Ca o definiţie, sistemul de calcul reprezintă un ansamblu de componente hardware (dispozitive) şi componente software (sistem de operare şi programe specializate) ce oferă servicii utilizatorului pentru coordonarea şi controlul executării operaţiilor prin intermediul programelor.

 Principiile de bază ale securităţii sistemelor informatice s-au schimbat relativ puţin în ultimii ani. Există două mari categorii – *protecţia la nivel fizic* (garduri, uşi cu încuietori, lacăte, etc.) şi *la nivel informaţional* (accesare prin intermediul unor dispozitive electronice şi/sau a unor aplicaţii software, a informaţiilor dintr-un sistem de clacul).



Fig. 1.1.1 Securitatea sistemelor informatice

Ca şi concepte distincte care tratează problema securităţii deosebim:

- securitatea bazată pe mai multe nivele – security in depth;
- securitatea implementată încă din faza de proiectare – security by design.

 Pentru a reduce riscurile de securitate în utilizarea şi administrarea sistemelor IT, cea mai bună strategie este cea pe ansamblu (security in depth). Aceasta presupune evaluarea pe ansamblu a infrastructurii IT şi clasificarea expunerii la riscuri de securitate. Pentru fiecare dintre riscurile identificate trebuie realizate planuri de măsuri, fie pentru reducerea expunerii la acele riscuri (mitigation), fie pentru reducerea impactului odată ce riscul s-a produs (contingency).

 La polul opus se află abordarea punctuală (limitată în a oferi protecţie doar la un anumit nivel), a implementării unui sistem specific de securitate, de exemplu antivirus sau detectarea accesului neautorizat (Intrusion Detection Systems – IDS). Deşi aceste sisteme sunt foarte utile în cadrul ariei specifice de aplicabilitate, această abordare lasă descoperite alte zone cu posibile breşe de securitate.

 Pentru a avea o abordare de ansamblu, trebuie pornit de la lucrurile elementare: uniformitatea infrastructurii din punct de vedere al sistemelor folosite, administrarea

centralizată, menţinerea la zi a sistemelor din punct de vedere al patch-urilor şi fix-urilor (pentru sistemele de operare şi aplicaţiile instalate), aplicarea unor configurări standard de securitate pe toate serverele şi staţiile de lucru, în funcţie de rolul funcţional al acestora precum şi realizarea unor proceduri standard de utilizare şi administrare.

Studiile arată că în medie 90% din breşele de securitate identificate nu sunt datorate problemelor tehnologice ci instalării şi configurării necorespunzătoare sau datorită nerespectării unor proceduri de utilizare şi administrare a sistemului. În multe cazuri, aceste proceduri nici nu există. Trebuie deci să privim problema pe ansamblu, adresând tehnologia, oamenii şi procedurile interne ale companiei/organizaţiei.

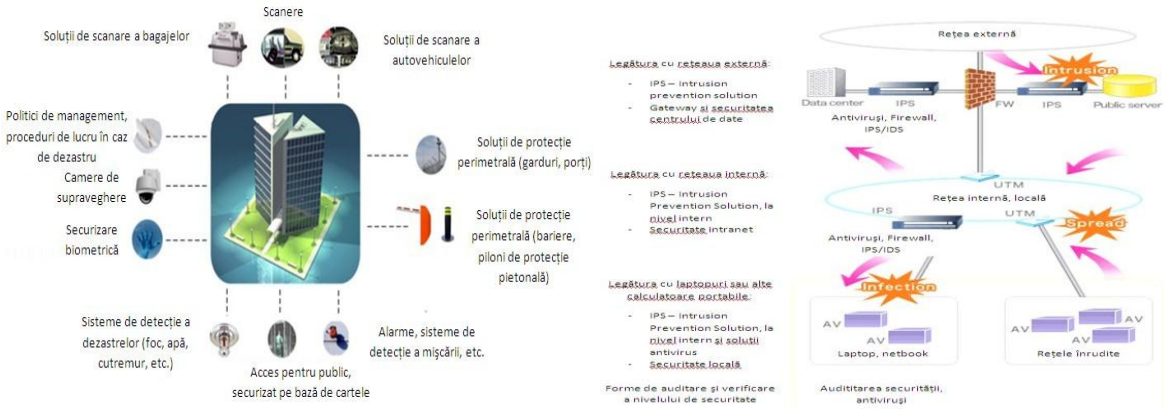


Fig. 1.1.2 Securitatea la nivel de acces perimetral şi la nivel informaţional

Securitatea trebuie să fie o caracteristică intrinsecă a sistemului. Un sistem sigur este unul bine proiectat, implementat, utilizat şi administrat.

Conceptul de „*security by design*” este foarte bun atunci când posibilităţile de implementare sunt justificate. De multe ori totuşi acest concept impune unele restricţii care limitează foarte mult utilizarea sa în arii diferite, metoda fiind folosită în zone speciale, foarte specializate (zone cu statut de importanţă majoră, ca de ex. reţelele de calculatoare care controlează traficul aerian, laboratoare de cercetare, etc.), zone în care accesul prin definiţie este foarte restrictiv.



Fig. 1.1.3 Exemplu de folosire al conceptului de „security by design” în viaţa de zi cu zi

Acest concept aplicat la „nivel software” generează un principiu de funcţionare al aplicaţiei cu restricţii foarte clare şi puternice – care de multe ori din pricina acestor limitări devine în scurt timp inutil.

„*In-depth security*” sau „*defence in depth*” este un principiu bazat pe mai multe „straturi” de securitate în vederea protejării sistemului sau reţelei din care face parte.

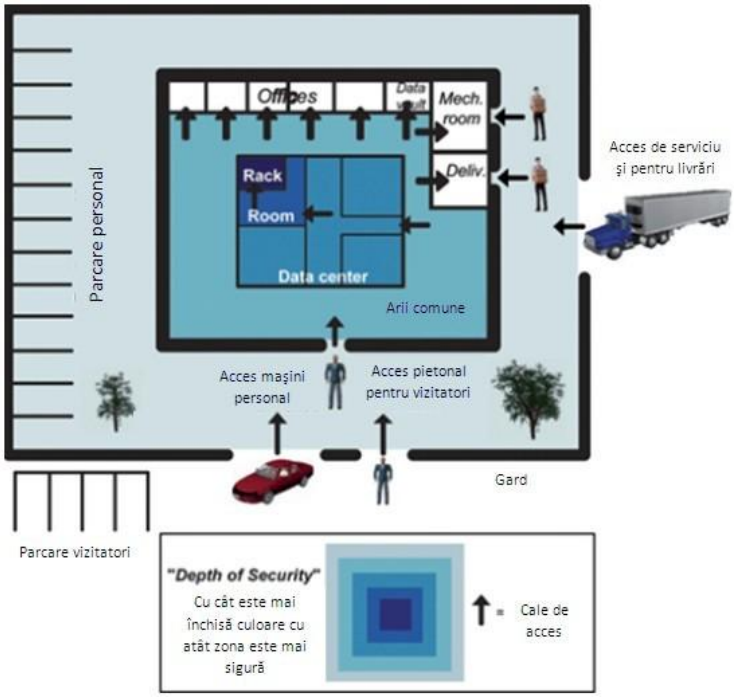


Fig 1.1.4. Evidenţierea conceptului de „Security in depth”

Trebuie să se înţeleagă că nu contează cât de de bun este fiecare „strat” – privit singular, există cineva mai deştept, cu resurse materiale şi temporale suficiente cât să treacă de acesta. Acesta este motivul pentru care practicile uzuale de securitate sugerează existenţa mai multor nivele de securitate sau pe scurt „in-depth security”.

Folosirea de nivele(layers) diferite de protecţie, de la diferiţi producători oferă o protecţie substanţial mai bună.

Folosind o securitate bazată pe diferite nivele de protecţie veţi fi protejaţi de majoritatea persoanelor răuvoitoare, cu excepţia celor mai deştepţi şi mai dedicaţi. Ca o regulă de bază (nivele minime de securitate instalate) se sugerează următoarele produse:

a) **firewall** – o barieră protectivă între calculator, reţeaua internă şi lumea din jur. Traficul din interior şi spre exterior este filtrat, restricţionat, blocând eventualele transmisii nenecesare. Folosind reguli stricte de acces la nivel de aplicaţii şi utilizatori, se poate îmbunătăţi substanţial securitatea sistemului şi a reţelei locale;

b) **antivirus** – un software instalat cu scopul clar de a te proteja de viruşi, viermi şi alte coduri maliţioase. Majoritatea aplicaţiilor antivirus monitorizează

traficul în fiecare moment, scanând în timp ce se navighează pe Internet sau scanând mesajele primite pe mail (cu tot cu ataşamente) şi periodic oferind posibilitatea rulării unei scanări la nivelul întregului sistem în căutarea de cod maliţios;



Fig. 1.1.5 Atenţie totuşi la aplicaţiile care se dau drept aplicaţii antivirus

c) **Intrusion Detection System (IDS) şi Intrusion Prevention System(IPS o varianta mai specială a IDS)** – un dispozitiv sau o aplicaţie folosit(ă) pentru a inspecta întregul trafic dintr-o reţea şi de a trimite mesaje de alertă utilizatorului sau administratorului sistemului cu privire la încercări neautorizate de acces. Principalele metode de monitorizare sunt cele bazate pe semnături şi cele bazate pe anomalii. Funcţie de metodele folosite IDS-ul poate rămâne la stadiul de a alerta utilizatori sau poate fi programat să blocheze automat traficul sau chiar programat să răspundă într-un anumit fel.

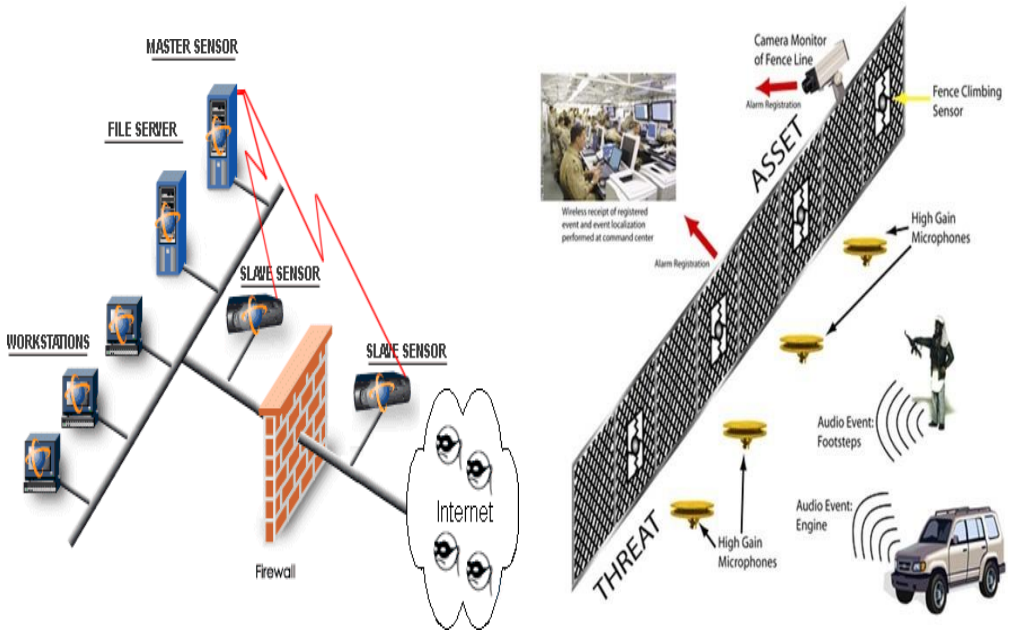


Fig. 1.1.6 IDS la nivel software şi hardware

Activitatea de învăţare 1.1.1 Securitatea la nivel fizic şi la nivel informatic

Obiectivul/obiective vizate:

- La sfârşitul activităţii vei fi capabil să identifici diferenţele dintre securitatea la nivel fizic şi securitatea la nivel informatic

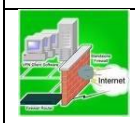
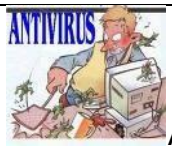
Durata: 20 min



Tipul activităţii: Învăţare prin categorisire

Sugestii : activitatea se poate desfăşura pe grupe sau individual

Sarcina de lucru: Având la dispoziţie următorul tabel, bifaţi corespunzător categoriei din care face parte fiecare imagine(text).

Imagine / text	Categoria din care face parte	
	Securitate la nivel fizic	Securitate la nivel informatic
 Lacăt		
 Uşă metalică		
 Firewall		
 Antivirus		
 Cabinet servere		
 Intrusion Detection System (IDS)		
 Router		

Pentru rezolvarea activităţii consultaţi Fişa de documentare 1.1