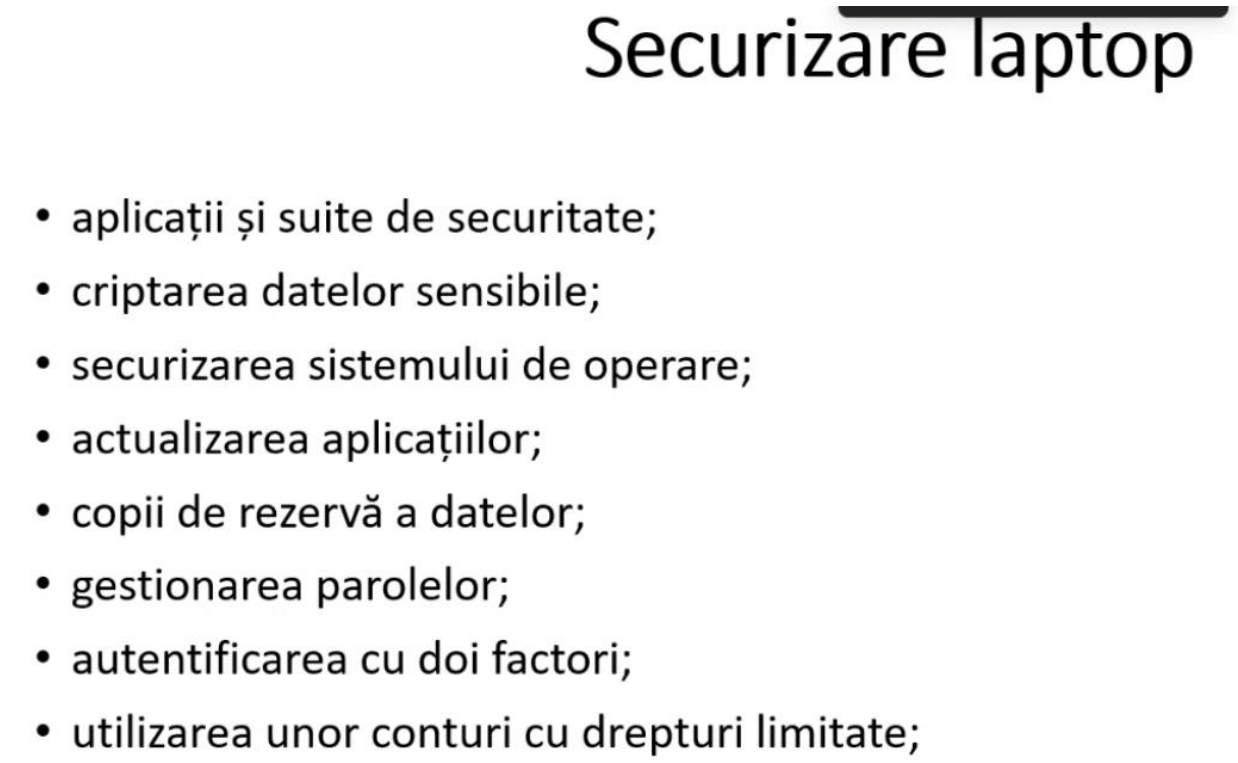
Reguli de bune practici

- Securizarea laptop
- Securizarea echipamente mobile
- Securizarea rețelei de calculatoare
- Programele malware
- Atacuri ce vizează conturile de email
- Atacuri ce vizează site-urile web
- Atacurile DoS și DDoS
- Atacuri ce vizează aplicațiile web
- Înșelăciuni pe rețelele de socializare
- Securitatea tranzacțiilor online
- Securitatea cardurilor de debit/credit
- Furtul de identitate
- Amenințări din interior



Securizare laptop

Avem 8 bullets care trebuie atinse, in primul rand trebuie sa avem grija sa instalam aplicatii anti-malware sau suite de securitate care sa fie complexe, performante, sa asigure protectia la cele mai recente tipuri de amenintari cibernetice. Aici, putem mentiona amenintarea cibernetica de tip ransomware.

Totodata, trebuie sa avem in vedere si actualizarea permanenta a bazei de date cu semnaturi malware, care este o conditie necesare pt detectia celor mai recente forme de amenintare.

Un alt aspect este cel legat de criptarea datelor sensibile, si aici se recomanda utilizarea unor aplicatii sau sisteme de operare care detin implementate facilitati pentru criptarea datelor sensibile la nivel de fisier individual/folder/drive logic.

Putem sa facem o conexiune, de exemplu, cu incidentul de securitate de la aerportul Heathrow din 2017-2018 cand un pasager a identificat un stick USB si pe acel memory stick era un plan de protectie antiterorista si beneficiarul era regina Angliei.

Acolo a fost o chestiune care, sa zicem, se incadreaza in zona breselor de securitate.

O alta masura de securitate pe care trebuie sa o avem in vedere este sa securizam sistemul de operare. Asta se realizaeaza prin repararea breselor de securitate si a erorilor hardware la nivelul tuturor componentelor sistemului de opereare prin aplicarea periodica automata sau manuala a

tuturor actualizarilor, cat si prin controlul accesului utilizatorilor la resurse, aici intelegand drepturile de accest la fisiere, servicii, sau aplicatii.

Actualizarea aplicatiilor. Utilizatorii trebuie sa activeze actualizare automata a tuturor aplicatiilor critice necesare, atat la nivel de sistem de opereare, cat si antivirus, firewall, sau sistem de detectie si preventie a intruziunii.

Important este sa vedem cum gestionam copiile de rezerva ale datelor pentru ca aceste date trebuie sa le salvam periodic, sa facem backup, sa le stocam pe suporturi dedicate, de incredere, sa le stocam in locuri sigure si criptate, ca sa evitam accesuri neautorizate. Aceste copii trebuie sa le pastram in mai multe locatii fizice, pentru a evita atat amenintarile naturale cat si amenintarile interne din cadrul companiei.

O alta masura de securitate este cea legata de gestionarea parolelor; in anumite situatii putem sa recomandam utilizarea unui manager de parole pentru a stoca parole complexe, unice, utilizate de calculator. Iar parolele pe care noi le folosim trebuie sa fie puternice, sa nu fie refolosite la mai multe conturi, schimbate in mod periodic.

Autentificarea cu doi factori este o metoda foarte eficienta si de actualitate care foloseste un dispozitiv suplimentar spre exemplu un token de securitate sau smartphone, pentru a confirma intr-un pas suplimentar identitatea persoanei care se autentifica.

Ultima masura, utilizarea unor conturi cu drepturi limitate, in locul unui cont de administrator. Toate lucrurile acestea vor bloca accesul la zone sensibile ale sistemului de operare, vor bloca implicit atacurile care vizeaza serviciile sistemului de opereare, fisierele, bibliotecile.

Securizare echipamente mobile

- activarea facilităților de protecție antifurt;
- sincronizarea datelor;
- actualizarea aplicațiilor;
- dezactivarea conexiunilor neutilizate;
- utilizarea aplicațiilor sigure;
- utilizarea unor medii de stocare verificate;
- distribuirea informațiilor personale;
- utilizarea cu precauție a codurilor QR(quick response);
- verificați drepturile de acces ale aplicațiilor;
- conexiuni securizate de date.

Avem in vedere activarea facilitatilor de protectie antifurt, functii de recunoastere faciala sau amprenta, deblocarea dispozitivului pe baza unor modele, sau PIN. Localizare echipament, blocare acces, stergere date de la distanta.

Sincronizarea datelor cu alte echipamente sau utilizarea servicii Cloud ne permite ca anumite informatii importante precum contacte, SMS-uri, documente importante, imagini, sa fie disponibile atunci cand echipamentul este pierdut sau furat.

Dezactivarea conexiunilor neutilizate. Daca nu avem nevoie de WiFi, bluetooth, bine sa dezactivam.

Utilizarea de aplicatii sigure – unele practici spun ca trebuie sa descarcam aplicatii numai din surse oficiale, sa nu permitem instalarea din surse nesigure.

Noi interactionam si cu medii de stocare, si aceste medii de stocare trebuie sa fie verificate inainte de a le conecta la telefonul mobil.

Distribuirea de informatii personale; partajarea unor informatii personale, cum ar fi, de exemplu, locatia geografica in timp real prin intermediul unor anumite aplicatii precum Waze poate permite unor terti sa monitorizeze traseele obisnuite – posibila tema de cercetare/lucrare de dizertatie: Distribuirea informatiilor personale prin intermediul echipamentelor mobile, prin intermediul aplicatiilor.

Utilizarea cu precautie a codurilor QR. Pot contine link-uri catre pagini web malitioase cu efecte daunatoare in ceea ce priveste securitatea datelor; extragerea locatiei geografice, accesul la fisiere, contacte, sau SMS-uri, sau transmiterea de mesaje nedorite prin email.

Verificati intotdeauna drepturile de acces ale aplicatiilor si utilizati conexiuni securizate de date. Evitati hotspot-urile wifi publice, si sa utilizati datele mobile ori de cate ori este posibil.

Un alt lucru pe care trebui sa il avem in vedere este cel legat de securizarea retelei de calculatoare. Aici se aplica toate lucrurile de inainte + lucruri dedicate. Securizarea fizica, controlul accesului, supraveghere video, personal de securitate, diverse metode, bariere, incuietor usi.

Securizarea server-elor si canalelor de cablu.

Firewall, de schimbat parole implicite, inclusiv pt dispoizitve IoT.

Tehnologii de comunicatii securizate la distanta: VPN-urile. Posibila tema dizertatie: cum este mai bine VPN -> TOR sau TOR -> VPN.

Am vorbit la un moment dat de autentifiare cifrata. Mesaj A->B cifrat + autentificat. Am la dispozitie o functie generica cifrare, o functie generica autentificare

Enc() Auth()

3 metode:

1) Iau mesaj, cifrez, transmit datele de autentificare a mesajului cifrat

   Enc(M) || Auth(Enc(M)) ← IPSEC

2) Iau mesajul, il concatenez, cu tag-ul de autentificare al mesajului clar, pun totul sub anvelopa cifrarii.

   Enc(M || Auth(M)) ← SSL

3) Transmit mesajul cifrat, concatenez cu tag-ul de autentificare al mesajului clar

   Enc(M) || Auth(M) ← SSH

Utilizarea celui mai mic privilegiu. Fiecare cont trebuie sa aiba alocate cele mai restrictive drepturi de acces, iar drepturile suplimentare vor fi alocate dupa necesitati. Evident, noi va trebui sa monitorizam ce fac utilizatorii in cadrul retelei, pentru a minimiza riscurile din interior.

O alta masura de securitate este cea referitoare la protectia retelelor wireless. Va trebui sa fitram echipamentele permise in retea pe baza adresei MAC, ascund identificatorul retelei (SSID), aloc adrese IP statice, sau reduc intervalul de adrese IP alocate dinamic.

Cresterea gradului de constientizare, aceasta retea este exploatata de utilizatori care pot face diverse activitati mai mult sau mai putin legitime.

Malware

- **Viruși:** se replică modificând alte programe de calculator prin introducerea propriului cod.
- **Troieni:** dau impresia că efectuează operațiuni legitime, când încearcă de fapt să exploreze vulnerabilitățile sistemului și să permită infractorilor cibernetici să acceseze sistemul în mod ilegal.
- **Viermi:** aplicații cu efecte distructive care infectează sistemul informatic și se propagă prin Internet.
- **Ransomware:** criptează sau blochează accesul la fișiere și solicită o răscumpărare pentru a elimina restricțiile.
- **Criptomineri:** aplicații care utilizează resursele informatice pentru a mina criptomonede pentru infractorii cibernetici.
- **Adware:** programe care transmit în mod agresiv reclame utilizatorilor.
- **Spyware:** captează diverse informații despre activitatea utilizatorilor pe Internet.
- **Rogueware:** programe care induc în eroare utilizatorii pentru a plăti pentru eliminarea unor infecții false detectate în sistemul de operare.

Malware – aplicatii sau script-uri concepute cu scopul de a modifica sau a sterge anumite date informatice, sa le deterioreze, sau sa restrictioneze accesul la calculatoare sau retea.

Malware

- soluție antivirus;
- aplicație de tip firewall;
- actualizare aplicații și sisteme de operare;
- dezactivare execuție automată a script-urilor pe site-uri web;
- utilizarea de aplicații de filtrare a e-mailurilor;
- evitarea utilizarii de conturi de administrator;
- copii de siguranță a datelor;
- instrumente avansate pentru detective;
- valorificarea jurnalelor;
- politica de securitate;
- reducerea accesului la funcțiile powershell;
- raportarea incidentelor de securitate

Solutie antivirus – detectam si eliminam programele malware in timp real.

Aplicatie tip firewall – inspectia traficului de pe paginile web, email-uri si aplicatii.

Actualizarea aplicatiilor si a sistemelor de operare; sa folosim aplicatii de filtrare a email-urilor.

Evitat de utilizat conturi admin pentru a preveni programele malware sa obtina privilegii de administrare;

Copii de siguranta a datelor pentru a face fata in cazul unei infectii reusite cu malware, va trebui sa restabilim informatia.

Trebuie sa monitorizam jurnalele (logs) utilizand diverse solutii de gestionare a incidentelor si evenimentelor de securitate.

SIEM – System Information Event Manager

Politici de securitate care specifica pasii care trebuie urmati in cadrul unei infectari.

Sa reducem accesul la functiile powrshell, si sa raportam aceste incidente de securitate, ca sa putem sa facem fata, sa le putem gestiona cum trebuie.

Atacuri care vizeaza conturile de e-mail

e-mail bombing: transmit in mod repetat email cu fisiere dim mari

e-mail spoofing: transmiterea email-uri cu adresa expeditorului modificata

e-mail spamming: continut comercial nesolicitat, atrage destinatarii sa acceseze site-ul si sa cumpere anumite produse

e-mail phishing – link-uri care fura date de autentificare, carduri…fac destinatarii sa furnizeze anumite informatii despre conturile bancare, carduri de credit, parole, detalii personale.

Masuri: dezactivarea executiei automate a codului

Solutii scuritate pentru email, filtre anti spam

Sa nu dam click pe link-uri si sa nu descarcam fisiere atasate daca nu suntem siguri de sursa email-ului

Auth in 2 pasi.

Parole utiizate complexe unice pt fiecare serviciu online

Tranzactii bancare.

Atacuri care vizeaza site-uri web, masuri generale: actualizare soft, fct avansate protectii endpoint, whitelist aplicatii, restricitonare continut web, folosind instrumente precum adblockers.

Monitorizare si filtrare adrese URL si fisiere daunatoare.

Atac DoS si DDoS, de regula practicate de grupari cu motivatii extremist/teroriste, incercari de a perturba traficul normal al unui server (serviciu/retea) prin suprasolicitarea sistemului tintit al infrastructurii cu volum mare de date.

Cum ne protejam? Sa intelegem serviciul, sa avem plan de raspuns, sa minimizam suprafata de atac, limitand optiunile eventualelor atacatori.

Nu expunem porturi, protocoale, aplicatii, de unde nu se asteapta nicio forma de comunicare.

Monitorizam, testam atacurile pentru a testa capacitatea de a raspunde.

Avem in vedere semne de ingrijorare, simptomele unui astfel de atac.

Pt aplicatii web:

Cross Site Scripting XSS – incarcarea unui script mailitos pe site-urile web pentru a fura date sau pentru a efectua anumite tipuri de daune

SQL injection – trimiterea codului distructiv printr-un formular de intrare

Solutii:

Security by design, aplicarea procedurilor de securitate inca din ciclul de dezvoltare

Sa utilizam niveluri de autorizare si mecanisme stricte de autentificare pt a preveni incalcarile de securitate.

Utilizare a tehnicilor de validare si izolare a intrarilor pt atacuri tip injectie.

Realizare evaluari risc/expunere inainte si in timpul procesului de dezvoltare al aplicatiei web.